ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Рекомендації щодо виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Ростислав ФАЙНА
(підпис)

Виконав: здобувач вищої освіти групи БСД-42
ФАЙНА Ростислав
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

DDoS – Distributed Denial of Service

DNS – Domain Name System

EDR – Endpoint Detection and Response

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

MFA – Multi-Factor Authentication

PCAP – Packet Capture

SIEM – Security Information and Event Management

SOAR – Security Orchestration Automation and Response

SOC – Security Operations Center

UEBA – User and Entity Behavior Analytics

XDR – Extended Detection and Response

ВСТУП

Актуальність дослідження. Для захисту корпоративних інформаційних ресурсів необхідно безперервно відстежувати та аналізувати стан мережі та кінцевих пристроїв, щоб швидко виявляти та реагувати на потенційні кіберзагрози. Цей підхід, що поєднує методи та засоби, процедури та аналітику, забезпечує захист від відомих і нових ризиків.

SIEM системи відіграють важливу роль у виявленні та реагуванні на загрози корпоративним інформаційним ресурсам. SIEM системи збирають дані з різних джерел, таких як журнали подій, мережевий трафік, дані з систем виявлення вторгнень, антивірусних програм та інших інструментів безпеки. SIEM системи використовують набір попередньо визначених правил, які описують відомі шаблони зловмисної активності. Ці правила застосовуються до зібраних даних для виявлення подій, які відповідають визначеним шаблонам. Кореляція подій дозволяє SIEM системі виявляти складні загрози, які можуть бути непоміченими при аналізі окремих подій.

Коли SIEM система виявляє загрозу, вона може автоматично генерувати сповіщення та повідомлення для фахівців з безпеки. За допомогою SIEM систем можна також автоматизувати певні дії з реагування на інциденти, такі як блокування IP-адрес, відключення облікових записів користувачів або ізоляція заражених систем. Це дозволяє скоротити час реагування на інциденти та мінімізувати потенційний збиток.

Ефективність SIEM систем залежить від якості визначених правил та кореляційних алгоритмів. Необхідно постійно оновлювати правила, щоб враховувати нові загрози та методи атак. Разом з цим, SIEM системи потребують кваліфікованих фахівців для їх налаштування та обслуговування.

Таким чином, SIEM системи на основі правил є потужним інструментом для захисту корпоративних інформаційних ресурсів від широкого спектру загроз та реагування на них, що визначає актуальність теми цієї кваліфікаційної роботи.

Основний зміст кваліфікаційної роботи становлять дослідження методів та засобів виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM.

Об'єкт дослідження – виявлення загроз корпоративним інформаційним ресурсам і реагування на них.

Предмет дослідження – методи та засоби виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM.

Мета роботи – розробити рекомендації щодо застосування методів та засобів виявлення загроз корпоративним інформаційним ресурсам і реагування на них.

Наукові завдання:

дослідити сутність проблеми виявлення загроз корпоративним інформаційним ресурсам і реагування на них;

проаналізувати підходи до виявлення загроз корпоративним інформаційним ресурсам і реагування на них;

проаналізувати існуючі рішення для виявлення загроз корпоративним інформаційним ресурсам і реагування на них;

проаналізувати методи та засоби виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM;

розкрити порядок виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано варіант системи виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ І РЕАГУВАННЯ НА НИХ

1.1. Дослідження проблеми виявлення загроз корпоративним інформаційним ресурсам і реагування на них

За даними IBM X-Force 2025 Threat Intelligence Index [1] виробничі організації продовжують зазнавати значного впливу атак, включаючи вимагання (29%) та крадіжку даних (24%), спрямованих на фінансові активи та інтелектуальну власність. Незважаючи на тенденцію до зниження кількості шкідливих програм, у 2024 році у виробництві спостерігалася найбільша кількість випадків програм-вимагачів, оскільки зловмисники продовжують використовувати застарілі технології в цій галузі.

Атаки на основі ідентифікації особи становлять 30% від загальної кількості вторгнень. Другий рік поспіль зловмисники застосовують більш приховані та наполегливі методи атак, причому майже кожна третя атака, яку X-Force спостерігає, використовується з використанням дійсних облікових записів. Зростання кількості фішингових електронних листів, що розповсюджують шкідливе програмне забезпечення для крадіжки інформації та фішинг облікових даних, підживлює цю тенденцію, що може бути пов’язано з тим, що зловмисники використовують штучний інтелект для масштабування атак [1].

Програми-вимагачі становлять 28% випадків шкідливого програмного забезпечення. Хоча програми-вимагачі становили найбільшу частку випадків шкідливого програмного забезпечення у 2024 році – 28%, X-Force спостерігала загалом зниження кількості випадків використання програм-вимагачів. Це вже третій рік поспіль, коли кількість випадків використання програм-вимагачів знижується. Це може бути частиною більшого зниження кількості атак програм-вимагачів, оскільки підприємства менш охоче платять викупи, а уряд посилює дії

проти груп, що займаються розповсюдженням програм-вимагачів [1].

4 з 10 найпопулярніших вразливостей, що найчастіше згадуються в даркнеті, повязані з витонченими зловмисниками. Усі 10 найпопулярніших вразливостей мали загальнодоступний код експлойту або були виявлені в активній експлуатації в реальних умовах, причому 60% з них активно експлуатувалися або мали загальнодоступний експлойт менш ніж через два тижні після розкриття до нульового дня. Це підвищує ризики для бізнесу, оскільки витончені зловмисники, включаючи державних суб'єктів, використовують анонімність даркнету для отримання нових інструментів та ресурсів [1].

У [1] відмічається, що кіберзлочинці, здатні змінювати форму, отримують більше доступу, легше переміщуються мережами та створюють нові форпости у відносній невідомості. Оснащені передовими інструментами, зловмисники все частіше використовують скомпрометовані облікові дані для входу, а не метод грубої сили злому. Збитки, які вони завдають, продовжують зростати, оскільки середня світова вартість витоку даних досягла рекордних 4,88 мільйона доларів у 2024 році.

Зі зростанням ефективності рішень для виявлення та реагування на кінцеві точки (EDR), що виявляють спроби проникнення через бекдор через фішинг, зловмисники перейшли до використання фішингу як тіньового вектора для доставки шкідливого програмного забезпечення-викрадача інформації. У 2024 році спостерігалося 84% зростання кількості інформаційних викрадачів, що постачалися через фішинг. Також спостерігалося 12% зростання облікових даних інформаційних викрадачів, що продаються в даркнеті, у порівнянні з минулим роком, що свідчить про збільшення їх використання [1].

Незважаючи на масштабність цих викликів, встановлено, що більшість організацій досі не мають плану дій у разі кіберкризи або посібників зі сценаріїв, які вимагають швидкого реагування. Потрібні швидкі та рішучі дії, щоб протидіяти швидшим темпам, з якими зловмисники, дедалі більше за допомогою штучного інтелекту, можуть здійснювати атаки, викрадати дані та використовувати вразливості [1].

На рисунку 1.1 показано найпопулярніші методи, що використовуються зловмисниками для отримання доступу до середовища жертви. Ці методи доступу описано відповідно до структури MITRE ATT&CK для підприємств, глобально доступної бази знань про тактику противника, складеної з реальних спостережень. Відсотки базуються на кількості випадків реагування на інциденти X-Force [1].

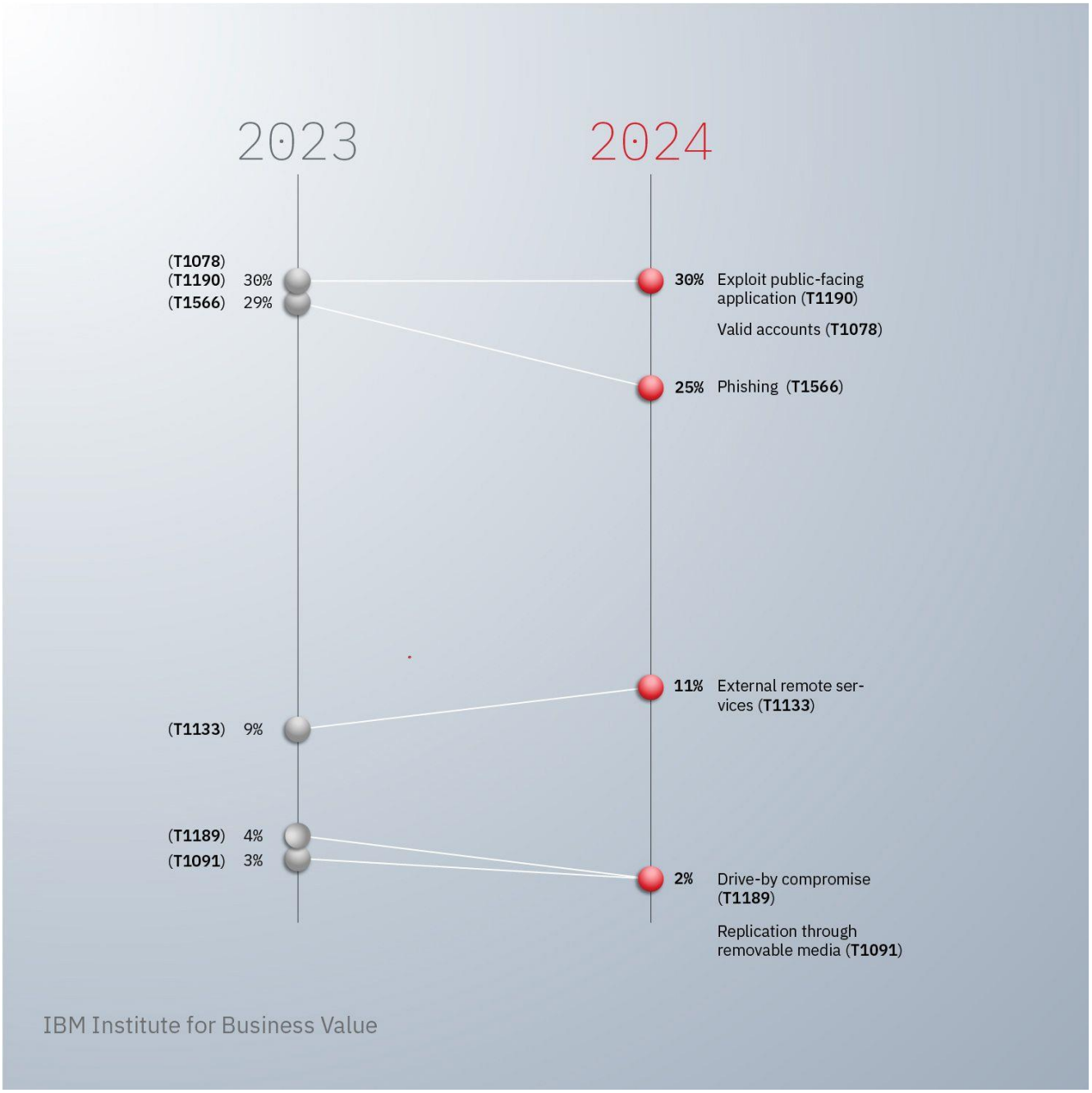

Рис. 1.1. Найпопулярніші методи, що використовуються зловмисниками для отримання доступу до середовища жертви [1]

Порівняно з попередніми роками, обсяг фішингових електронних листів, що

розповсюджують стійке шкідливе програмне забезпечення з бекдором, значно зменшився. Масові розповсюджувачі шкідливого програмного забезпечення, що призводять до атак програм-вимагачів, включаючи Emotet, TrickBot, IcedID, Qakbot, Gozi та Pikabot, значною мірою зникли з поля зору. *Розгортання стійкого шкідливого програмного забезпечення на кінцевій точці через електронну пошту набагато частіше виявляється рішеннями EDR, що змушує зловмисників адаптувати стратегії та зосередитися на ідентифікації.* Це проявилося у збільшенні використання інформаційних викрадачів та переході до фішингу облікових даних [1].

Фреймворки ботів Infostealer дозволяють зловмисникам розробляти поведінку інфостелерів та створювати серверні панелі керування, куди інфостелери надсилають дані. Ми спостерігали зростання кількості інфостелерів, що надсилаються в середньому через фішингові електронні листи на тиждень, на 84% порівняно з 2023 роком. Попередні дані за 2025 рік свідчать про ще більше зростання тижневого обсягу на 180% порівняно з 2023 роком [1].

Використовуючи інфостелери, зловмисники можуть швидко викрасти облікові дані до їх виявлення, не використовуючи постійний бекдор як початковий плацдарм. Найпоширенішим шкідливим програмним забезпеченням-викрадачами інформації, що поширювалося безпосередньо через фішинг, був AgentTesla, за ним ішли FormBook, SnakeKeylogger та PureLogs Stealer [1].

У [1] відмічається, що організації не можуть реально блокувати PDF-файли та URL-адреси в електронних листах, оскільки вони використовуються повсюдно в повсякденній діяльності. Крім того, організації не можуть блокувати легітимні хмарні хостингові сервіси при фішінгових атаках.

Єдиний спосіб уникнути цього – використовувати чутливу до часу інформацію про загрози для блокування URL-адрес, що використовуються зловмисно протягом короткого періоду часу, та покладатися на багаторівневий захист для зменшення впливу, якщо користувачі клюються на фішингову електронну пошту. Це означає використання EDR для виявлення шкідливого програмного забезпечення, що краде інформацію, та використання ключів

доступу та багатофакторної автентифікації (MFA) для зменшення ризику кампаній з викрадання облікових даних Єдиним ефективним способом протидії масштабам цих атак буде використання інструментів штучного інтелекту та автоматизації [1].

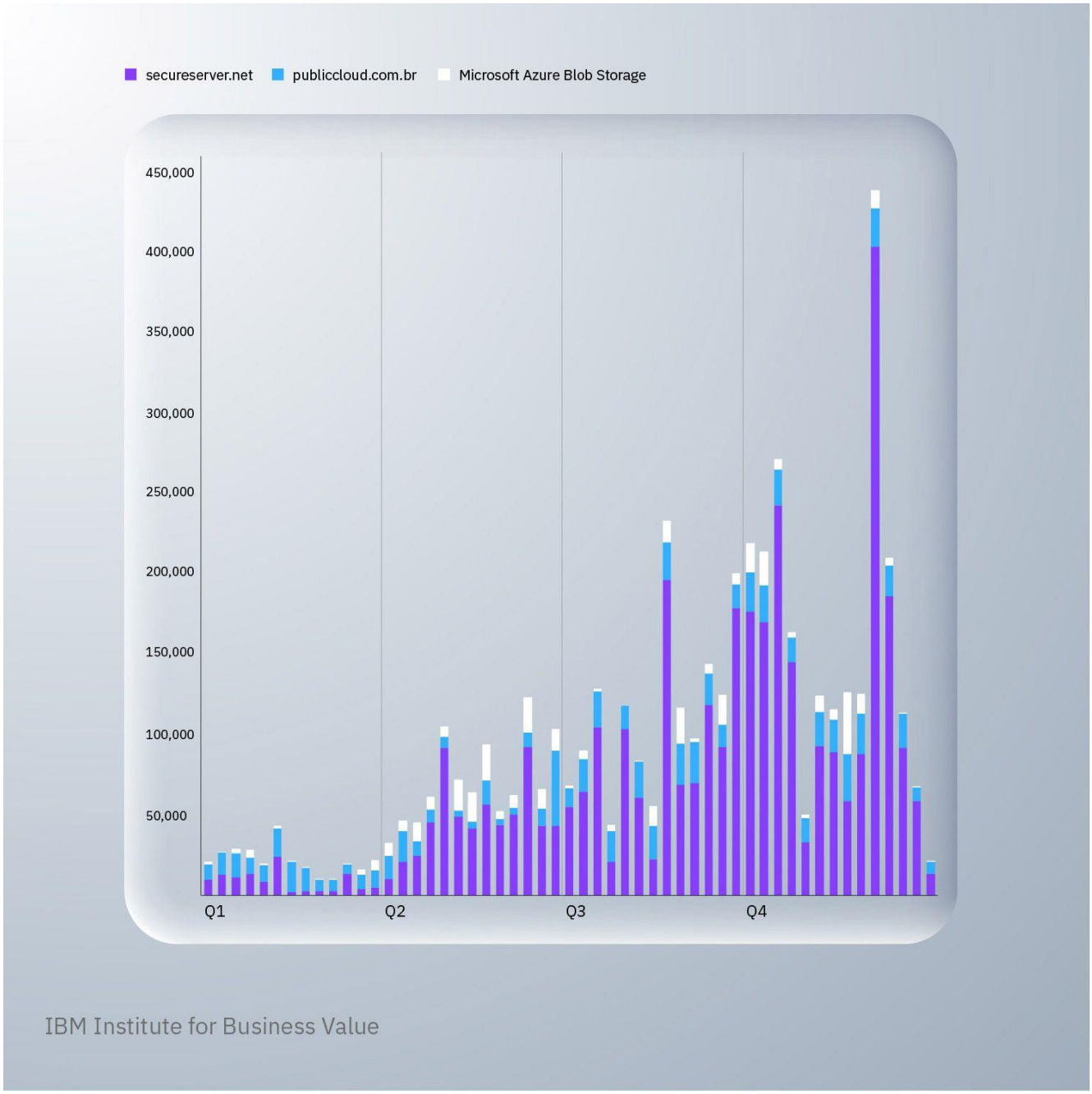

Рис. 1.2. Частота спаму та шкідливого програмного забезпечення, розміщених у великих публічних хмарних середовищах [1]

На рисунку 1.2 показано кількість спостережуваних спам-повідомлень електронної пошти з посиланнями на певного постачальника хмарного хостингу.

Зловмисники намагаються маскувати шкідливу активність, використовуючи популярні хмарні хостингові сервіси. Хмарні хостингові сервіси secureserver.net (фіолетовий), publiccloud.com.br, що належать Locaweb Serviços de Internet (синій), та Microsoft Azure Blob Storage (білий) активно зловживаються як засіб розповсюдження фішингових сайтів облікових даних та банківських троянських шкідливих програм, таких як Grandoreiro, Mekotio та Guildma. ПРИМІТКА. Використання конкретного хмарного постачальника для розміщення шкідливого контенту не свідчить про недолік безпеки платформи, але ілюструє, де зловмисники вирішують розміщувати шкідливе програмне забезпечення. Часто зловмисники обирають відомих та визнаних постачальників, щоб обдурити жертв, приховуючи зловмисну діяльність серед інших легітимних робочих навантажень, що ускладнює ідентифікацію та ізоляцію цієї діяльності [1].

30% інцидентів, на які відреагувала X-Force у 2024 році, стосувалися експлуатації загальнодоступних додатків [1]. Для багатьох організацій це посилюється проблемами з управлінням патчами вразливостей. Крім того, у 25% цих випадків ми спостерігали активне сканування після компрометації, тобто зловмисники використовували інструменти сканування вразливостей для виявлення додаткових вразливостей, отримання додаткового доступу та нестандартного просування в скомпрометованому середовищі [1].

Зловмисники використовують відомі вразливості в поширених додатках та інфраструктурних сервісах, і вектор атаки полягає лише в дії на основі цих знань. Боти та інструменти автоматизації, отримані в даркнеті, можуть бути спрямовані на ключові інфраструктурні додатки та сервіси організації [1].

На жаль, для кіберзахисників не бракує вразливостей для використання. З 1993 року ми класифікували понад 300 000 унікальних вразливостей. Серед них майже 65 000 вразливостей із загальнодоступним експлойтом, багато з яких зловмисники використовували для компрометації середовища. Іншими словами, майже чверть усіх вразливостей мають повязаний експлойт, що використовується як зброя, який можуть використовувати зловмисники [1].

На рисунку 1.3 показано кількість виявлених уразливостей у реальному

часі. База даних вразливостей IBM X-Force є однією з найстаріших і найбільших баз даних вразливостей у світі [1].

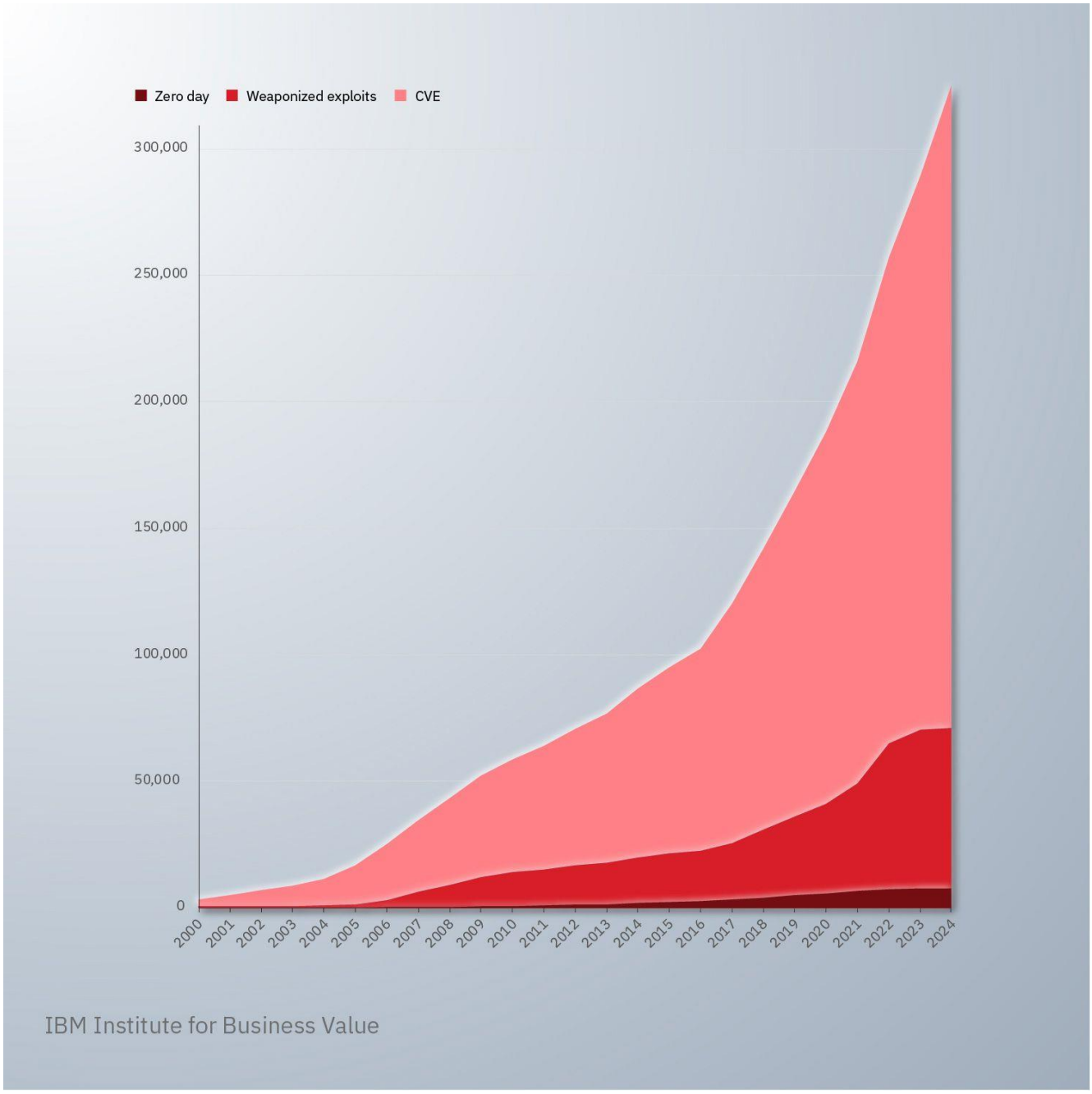

Рис. 1.3. Зростання вразливостей, експлойтів, що перетворюються на зброю, та нульових днів [1]

Також слід зазначити, що кількість вразливостей швидко зросла за останні вісім років і зросла втричі. Це можна пояснити багатьма факторами. Можливо, найімовірнішим є зростання залежності від спільної хмарної інфраструктури та сервісів. Атака на спільну хмарну інфраструктуру – це цінна можливість для

зловмисників розгортати шкідливе програмне забезпечення у великих масштабах та розширювати свій потенціал для порушення роботи. Це ще одна переконлива причина, чому принципи нульової довіри, такі як сегментація мережі, є важливими для кіберзахисту. Ізолюючи робочі навантаження, обмежується потенційний радіус вибуху атак [1].

1.2. Аналіз підходів до виявлення загроз корпоративним інформаційним ресурсам і реагування на них

Microsoft [2] визначає виявлення загроз та реагування на них як процес кібербезпеки, який дозволяє виявити кіберзагрози цифровим активам організації та вжити заходів для їх якомога швидшого пом’якшення.

Для вирішення кіберзагроз та інших проблем безпеки багато організацій створюють центр операцій безпеки (Security Operations Center, SOC), який є централізованою функцією або командою, відповідальною за покращення стану кібербезпеки організації та запобігання, виявлення та реагування на загрози. Окрім моніторингу та реагування на поточні кібератак, SOC також виконує проактивну роботу з виявлення нових кіберзагроз та вразливостей організації. Більшість команд SOC, які можуть бути на місці або передані на аутсорсинг, працюють цілодобово, сім днів на тиждень [2, 3].

SOC використовує дані розвідки про загрози та технології для виявлення спроб, успішних або поточних порушень. Після виявлення кіберзагрози команда безпеки використовуватиме інструменти виявлення та реагування на загрози, щоб усунути або пом’якшити проблему [2, 3].

Існує чотири типи виявлення загроз: конфігурація, моделювання, індикатор та поведінка загрози. Конфігурація ідентифікує загрози, знаходячи відхилення від коду на основі відомої архітектури. Моделювання – це математичний підхід, який визначає «нормальний» стан і позначає будь-які відхилення як загрози [4].

Індикатори використовуються для позначення файлів або даних як хороших або поганих на основі елементів інформації, які ідентифікують ці стани.

Поведінка загроз кодує поведінку зловмисників для виявлення, спираючись на аналіз дій, виконаних у мережі або додатку. Кожен тип виявлення загроз чудово працює в різних сценаріях. Знання потреб конкретного бізнесу може допомогти визначити, які інструменти виявлення загроз використовувати [4].

Виявлення загроз та реагування на них зазвичай включає такі етапи [2, 3]:

виявлення. Інструменти безпеки, які моніторять кінцеві точки, ідентифікаційні дані, мережі, програми та хмари, допомагають виявляти ризики та потенційні порушення. Фахівці з безпеки також використовують методи полювання на кіберзагрози для виявлення складних кіберзагроз, які уникають виявлення;

розслідування. Після виявлення ризику SOC використовує штучний інтелект та інші інструменти, щоб підтвердити реальність кіберзагрози, визначити, як вона сталася, та оцінити, які активи компанії постраждали;

стримування. Щоб зупинити поширення кібератаки, команди кібербезпеки та автоматизовані інструменти ізолюють заражені пристрої, ідентифікаційні дані та мережі від решти активів організації;

викорінення. Команди усувають першопричину інциденту безпеки з метою повного усунення зловмисника з середовища. Вони також усувають вразливості, які можуть наразити організацію на ризик аналогічної кібератаки;

відновлення. Після того, як команди достатньо впевнені, що кіберзагрозу або вразливість усунуто, вони знову підключають усі ізольовані системи до мережі;

надання звіту. Залежно від серйозності інциденту, групи безпеки задокументують та проінформують керівників, виконавчих директорів та/або раду директорів про те, що сталося та як проблему було вирішено;

зменшення ризиків. Щоб запобігти повторенню подібного порушення та покращити реагування в майбутньому, команди вивчають інцидент та визначають зміни, які потрібно внести до середовища та процесів.

Щоб випередити зростання кількості кібератак, організації використовують моделювання загроз для визначення вимог безпеки, виявлення вразливостей і ризиків, а також визначення пріоритетів усунення наслідків. Використовуючи

гіпотетичні сценарії, SOC намагається проникнути в свідомість кіберзлочинців, щоб вони могли покращити здатність організації запобігати інцидентам безпеки або пом’якшувати їх наслідки. Структура MITRE ATT&CK є корисною моделлю для розуміння поширених методів і тактик кібератак [2].

Моделювання загроз – це корисна стратегія для виявлення та реагування на кіберзагрози. MITRE ATT&CK, глобально доступна база знань про методи та тактики зловмисників, є прикладом моделювання загроз. Кожен процес моделювання загроз повинен застосовувати розвідку про загрози, визначати активи та можливості пом’якшення наслідків, оцінювати ризики та виконувати картографування загроз. Інші методи моделювання загроз включають Загальну систему оцінювання вразливостей (Common Vulnerability Scoring System) та Візуальну, Гнучку та Просту загрозу (Visual, Agile та Simple Threat) [4].

Багаторівневий захист вимагає інструментів, які забезпечують безперервний моніторинг середовища в режимі реального часу та виявляють потенційні проблеми безпеки. Рішення також повинні перетинатися, щоб у разі порушення одного методу виявлення, другий виявив проблему та повідомив команду безпеки. Рішення для виявлення кіберзагроз використовують різноманітні методи для виявлення загроз, зокрема:

виявлення на основі сигнатур. Багато рішень безпеки сканують програмне забезпечення та трафік, щоб виявити унікальні сигнатури, пов’язані з певним типом шкідливого програмного забезпечення;

виявлення на основі поведінки. Щоб допомогти виявляти нові та нові кіберзагрози, рішення безпеки також шукають дії та поведінку, поширені під час кібератак;

виявлення аномалій. Штучний інтелект та аналітика допомагають командам зрозуміти типову поведінку користувачів, пристроїв та програмного забезпечення, щоб вони могли виявити щось незвичне, що може свідчити про кіберзагрозу.

Хоча програмне забезпечення є критично важливим, люди відіграють не менш важливу роль у виявленні кіберзагроз. Окрім сортування та розслідування системних сповіщень, аналітики використовують методи полювання на

кіберзагрози для проактивного пошуку ознак компрометації або шукають тактики, методи та процедури, які вказують на потенційну загрозу. Ці підходи допомагають SOC швидко виявляти та зупиняти складні, просунуті атаки.

Після виявлення достовірної кіберзагрози, реагування на загрозу включає будь-які дії, які вживає SOC для її стримування та усунення, відновлення та зменшення ймовірності повторення подібної атаки. Багато компаній розробляють план реагування на інциденти, щоб допомогти їм під час потенційного порушення, коли організованість та швидкі дії є критично важливими. Гарний план реагування на інциденти включає посібники з покроковими інструкціями для конкретних типів загроз, ролей та обов'язків, а також план комунікації [2].

Організації використовують різноманітні інструменти та процеси для ефективного виявлення загроз та реагування на них, а саме [2]:

рішення розширеного виявлення та реагування (XDR) допомагають центрам захисту даних (SOC) спростити весь життєвий цикл запобігання, виявлення та реагування на кіберзагрози. Ці рішення контролюють кінцеві точки, хмарні програми, електронну пошту та ідентифікаційні дані. Якщо рішення XDR виявляє кіберзагрозу, воно сповіщає команди безпеки та автоматично реагує на певні інциденти на основі критеріїв, визначених SOC;

рішення для управління інформацією та подіями безпеки (SIEM). Отримання уявлення про все цифрове середовище – це перший крок до розуміння ландшафту загроз. Більшість команд SOC використовують рішення для управління інформацією та подіями безпеки (SIEM), які агрегують та співвідносять дані між кінцевими точками, хмарами, електронною поштою, програмами та ідентифікаторами. Ці рішення використовують правила виявлення та схеми дій для виявлення потенційних кіберзагроз шляхом співвіднесення журналів та сповіщень. Сучасні SIEM також використовують штучний інтелект для ефективнішого виявлення кіберзагроз та включають зовнішні канали розвідки про загрози, щоб вони могли виявляти нові кіберзагрози;

рішення для виявлення та реагування на кінцеві точки (EDR) – це попередня версія рішень XDR, орієнтованих лише на кінцеві точки, такі як комп’ютери,

сервери, мобільні пристрої, Інтернет речей. Як і рішення XDR, коли виявляється потенційна атака, ці рішення генерують сповіщення та, на певні добре зрозумілі атаки, реагують автоматично. Оскільки рішення EDR орієнтовані лише на кінцеві точки, більшість організацій переходять на рішення XDR;

рішення для оркестрації, автоматизації та реагування на кіберзагрози (SOAR) допомагають спростити виявлення та реагування на кіберзагрози, об'єднуючи внутрішні та зовнішні дані й інструменти в одному централізованому місці. Вони також автоматизують реагування на кіберзагрози на основі набору попередньо визначених правил;

виявлення загроз ідентифікації та реагування на них. Оскільки зловмисники часто націлені на співробітників, важливо запровадити інструменти та процеси для виявлення та реагування на загрози ідентичності організації. Ці рішення зазвичай використовують аналітику поведінки користувачів та сутностей (UEBA) для визначення базової поведінки користувачів та виявлення аномалій, які становлять потенційну загрозу;

розвідка про загрози. Щоб отримати повне уявлення про ландшафт кіберзагроз, SOC використовують інструменти, які синтезують та аналізують дані з різних джерел, включаючи кінцеві точки, електронну пошту, хмарні додатки та зовнішні джерела розвідки про загрози. Аналітика з цих даних допомагає командам безпеки готуватися до кібератаки, виявляти активні кіберзагрози, розслідувати поточні інциденти безпеки та ефективно реагувати;

управління вразливостями – це безперервний, проактивний і часто автоматизований процес, який контролює комп'ютерні системи, мережі та корпоративні програми на наявність слабких місць безпеки. Рішення з управління вразливостями оцінюють вразливості за серйозністю та рівнем ризику й надають звіти, які SOC використовує для усунення проблем;

кероване виявлення та реагування. Не всі організації мають ресурси для ефективного виявлення кіберзагроз та реагування на них. Керовані служби виявлення та реагування допомагають цим організаціям поповнити свої команди безпеки інструментами та людьми, необхідними для виявлення загроз та

належного реагування.

Різні підходи до управління інформацією про загрози можуть включати використання SIEM, XDR або інструментів оркестрації безпеки, автоматизації та реагування (SOAR). Інструмент SIEM, ймовірно, надасть детальну інформацію про подію безпеки, тоді як система SOAR корисна для збору даних та ініціювання автоматизованої відповіді на атаку. Їхні можливості працюють разом. XDR також використовує дані SIEM, але його можливості реагування набагато масштабніші, ніж у SOAR (рисунок 1.4) [5].

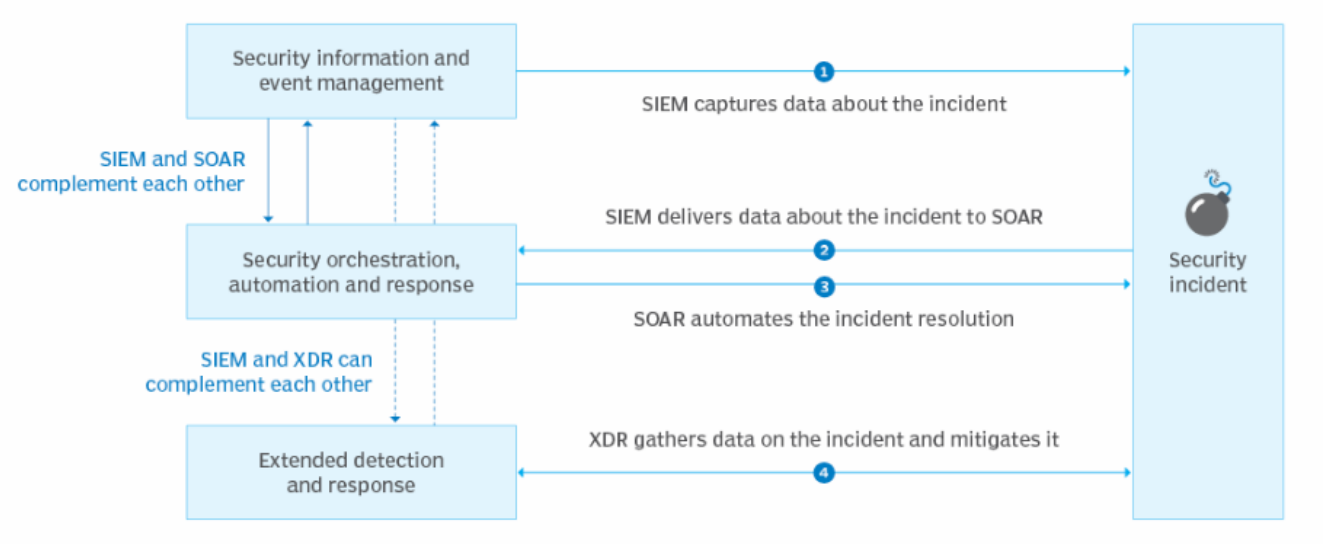

Рис. 1.4. Сумісне використання інструментів SIEM, XDR та SOAR [5]

Ще одним постійним розвитком у сфері виявлення та реагування на загрози є ширше використання аутсорсингових послуг. Gartner прогнозує, що до 2025 року цілих 50% підприємств використовуватимуть сторонні послуги принаймні для частини своєї роботи з виявлення та реагування на загрози. Вибираючи керовану службу безпеки, організації повинні ретельно враховувати сильні сторони постачальника, запитувати про глобальне покриття та визначати, які показники звітності будуть надаватися [5].

Отже, виявлення загроз та реагування на них – це критично важлива функція, яку всі організації можуть використовувати для пошуку та усунення кіберзагроз, перш ніж вони завдадуть шкоди.

1.3. Аналіз існуючих рішень для виявлення загроз інформаційним системам організацій

Рішення SIEM надають організаціям передові можливості криміналістики та дозволяють їм реконструювати місця злочину. Вони відстежують цифрові сліди, виявляючи поведінку злочинців, відхилення та тонкощі в мережевих рухах, а також запускають сповіщення для попередження служб безпеки. По суті, інструменти SIEM є агрегаторами даних; вони допомагають компаніям централізувати журнали та події безпеки. Аналізуючи зібрані дані, організації можуть виявляти приховані вразливості та запобігати майбутнім порушенням. Згенеровані звіти та аналітику можна зіставити з певними наборами правил. А організації можуть отримувати таку деталізовану інформацію, як вони хочуть, зосереджуючись на ключових показниках та досліджуючи сповіщення [10].

SIEM – це тип програмного забезпечення, яке збирає, контролює та аналізує дані, пов’язані з безпекою, з різних джерел, таких як мережеві пристрої, сервери, додатки та системи. Воно забезпечує видимість та аналітику подій, загроз та інцидентів, пов’язаних з безпекою, у режимі реального часу, дозволяючи організаціям виявляти, реагувати та запобігати порушенням безпеки [3, 10-12].

SIEM використовують попередньо визначені правила для генерації сповіщень та надають можливості реагування на інциденти. Найкраще програмне забезпечення SIEM сьогодні еволюціонувало та включає аналітику поведінки користувачів та об’єктів (UEBA). Вони стають основним елементом для сучасних команд SOC для різних сценаріїв моніторингу безпеки та управління відповідністю вимогам [3, 10-12].

SIEM є важливими для організацій, щоб виявляти, реагувати та запобігати загрозам безпеці в сучасному складному та динамічному ландшафті загроз. Ось кілька причин, чому нам потрібні інструменти SIEM [10]:

збільшення кіберзагроз. Кількість та складність кіберзагроз значно зросли, що ускладнює для організацій своєчасне виявлення загроз та реагування на них. Інструменти SIEM допомагають організаціям випереджати ці загрози,

забезпечуючи видимість та аналітику в режимі реального часу;

обсяг даних журналів. Обсяг даних журналів, що генеруються різними системами, програмами та пристроями, вражає. SIEM допомагають організаціям розібратися в цих даних, виявляючи закономірності, аномалії та потенційні загрози безпеці;

обмежені ресурси безпеки. Багато організацій мають обмежені ресурси безпеки, включаючи персонал, бюджет і технології. SIEM допомагають організаціям максимізувати свої ресурси безпеки, забезпечуючи централізовану платформу для моніторингу та реагування на загрози безпеці;

вимоги до відповідності. Організації підлягають різним вимогам до відповідності, таким як GDPR, HIPAA та PCI-DSS, які вимагають збору, зберігання та аналізу даних журналів. SIEM допомагають організаціям дотримуватися цих вимог до відповідності, надаючи журнали аудиту, можливості зберігання журналів та звітності;

відображення в режимі реального часу. SIEM забезпечують видимість подій, пов’язаних із безпекою, в режимі реального часу, дозволяючи організаціям швидко виявляти загрози та реагувати на них. Це знижує ризик порушень безпеки та мінімізує вплив на бізнес-операції;

покращене реагування на інциденти. SIEM надають службам реагування на інциденти інструменти та функції, необхідні для ефективного розслідування та реагування на інциденти безпеки. Це включає такі функції, як оповіщення, сповіщення та відстеження інцидентів;

зменшення часу простою. SIEM допомагають організаціям скоротити час простою, швидко виявляючи та реагуючи на інциденти безпеки, мінімізуючи вплив на бізнес-операції;

покращений рівень безпеки. SIEM допомагають організаціям покращити свій рівень безпеки, надаючи комплексне уявлення про події, пов’язані з безпекою, що дозволяє їм виявляти та усувати вразливості та слабкі місця;

економія коштів. SIEM можуть допомогти організаціям знизити витрати, пов'язані з порушеннями безпеки, шляхом швидкого виявлення та реагування на

загрози, зменшуючи потребу в дорогих заходах з відновлення.

інтеграція з іншими інструментами безпеки. SIEM можуть інтегруватися з іншими інструментами безпеки, такими як брандмауери, системи виявлення вторгнень та антивірусне програмне забезпечення, забезпечуючи комплексне рішення безпеки.

Як SIEM наступного покоління, *Exabeam Fusion* – це хмарне рішення, яке використовує поведінковий підхід для виявлення, розслідування та реагування на загрози (TDIR). Агрегуючи всі відповідні події та відсіюючи незаконні події, Fusion SIEM підвищує продуктивність аналітиків та виявляє загрози, пропущені іншими інструментами. Це покращує показники виявлення та час реагування, а також гарантує, що всі сповіщення будуть враховані, навіть ті, що надходять від «шумних» систем, які генерують багато сповіщень [11].

Крім того, Fusion SIEM інтегрований з рішенням для оркестрації та автоматизації безпеки (SOAR), яке забезпечує автоматизоване реагування на інциденти. Це дозволяє автоматично (або напівавтоматично, якщо бажано) реагувати майже на будь-яку загрозу в режимі реального часу. Приписувані робочі процеси та попередньо підготовлений контент для сценаріїв використання (зовнішні загрози, скомпрометовані інсайдери та зловмисні інсайдери) забезпечують успішне вирішення проблем із загрозами та автоматизацію реагування. Fusion SIEM також забезпечує хмарне сховище журналів, швидкий та керований пошук, а також вичерпну звітність про відповідність, яка очікується від будь-якої сучасної SIEM (рисунок 1.5) [11].

IBM QRadar SIEM дозволяє переглядати корпоративну IT-інфраструктуру в режимі реального часу. Це модульна архітектура, яка сприяє виявленню та визначенню пріоритетів загроз. Вона підтримує кілька протоколів ведення журналу та пропонує різні опції налаштування, а також високоякісну аналітику. Рішення надає магазин додатків, де клієнти можуть завантажувати додатковий контент IBM та сторонніх розробників для використання з QRadar (рисунок 1.6) [11].

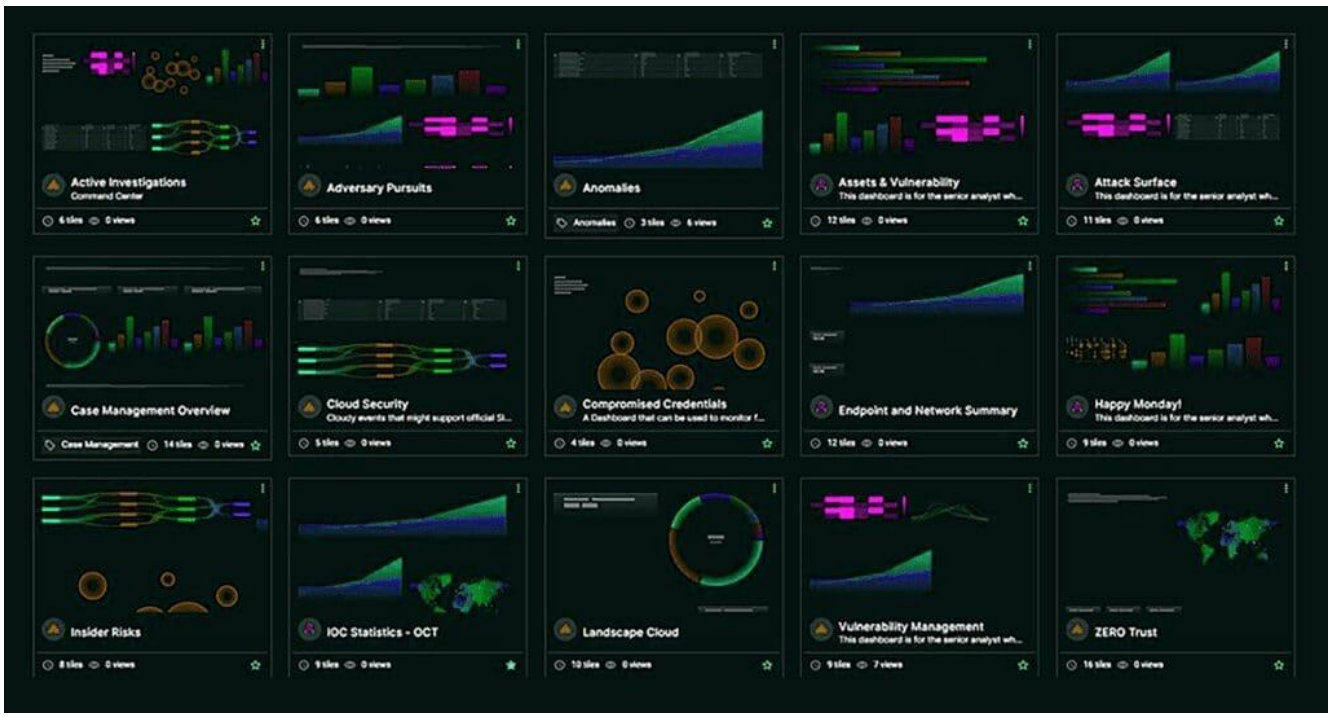

Рис. 1.5. Інструментальна панель Exabeam Fusion

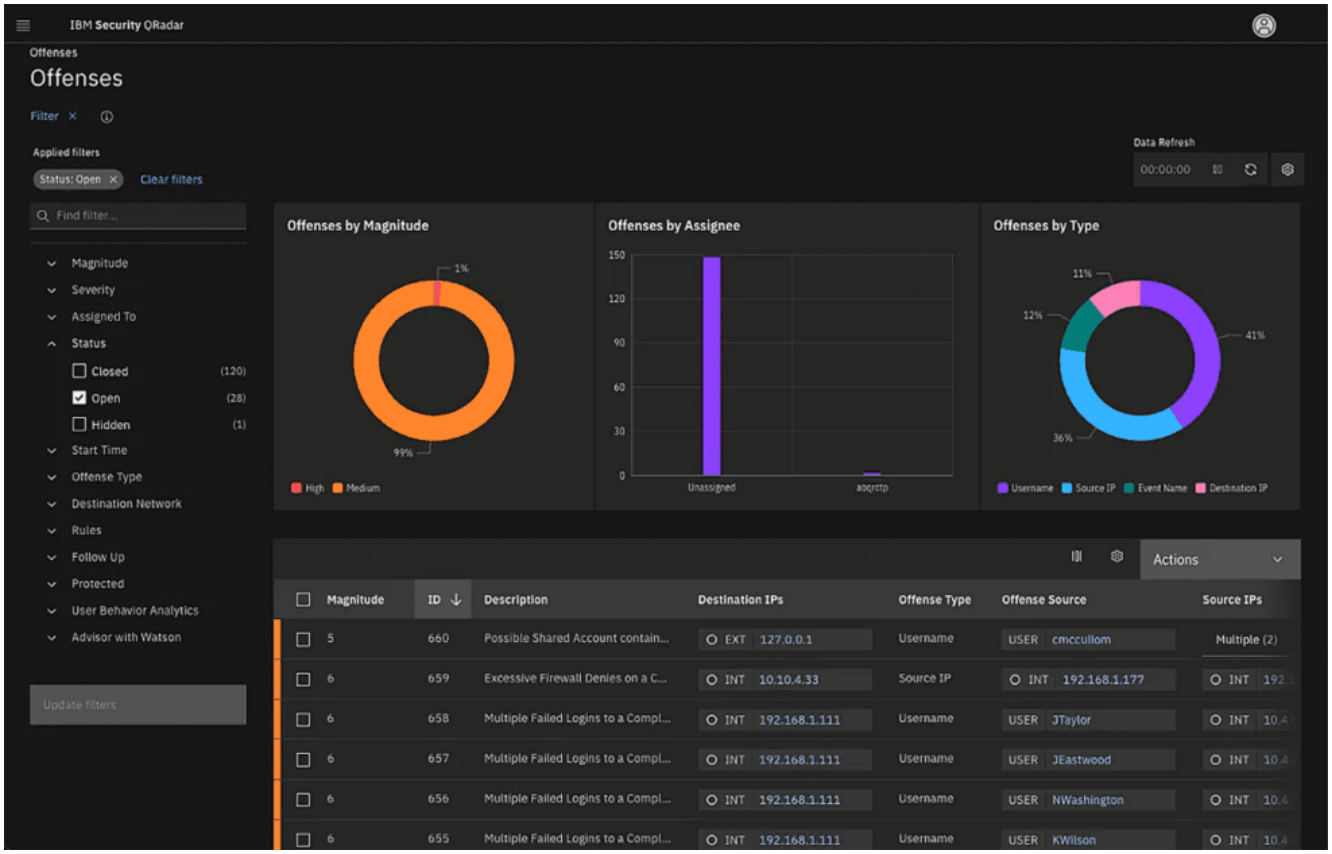

Рис. 1.6. Інтерфейс IBM QRadar SIEM

Однак, IBM QRadar має деякі недоліки, зокрема відносно високу вартість (і

складну модель ціноутворення), а також вимогу до функцій співпраці, таких як інструменти чату та покращене управління активами. Крім того, QRadar має слабкі можливості UEBA, які є базовим компонентом SIEM наступного покоління. Іншими недоліками є те, що в розподілених середовищах оновлення можуть бути складними та вимагати значних зусиль, оскільки часто існує обмежена підтримка продукту (хоча ви можете придбати оновлену підтримку). Продукт має обмежені можливості звітності, які необхідно доповнювати скриптами, розробленими зовнішніми розробниками [11].

Microsoft Azure Sentinel – це потужне SIEM-рішення, яке є відносно новим на ринку, оскільки Microsoft випустила платформу наприкінці 2019 року. Це дуже популярний вибір для клієнтів, які вже мають інвестиції в безпеку та IT від Microsoft і хочуть об'єднати їх в одному інформаційному центрі. Воно також пропонує унікальну модель ліцензування «оплата за використання», яка відповідає бюджетним вимогам малого та середнього бізнесу, а також може бути привабливою для великих підприємств. Azure Sentinel також відомий своїм безперебійним процесом адаптації даних (рисунок 1.7) [11].

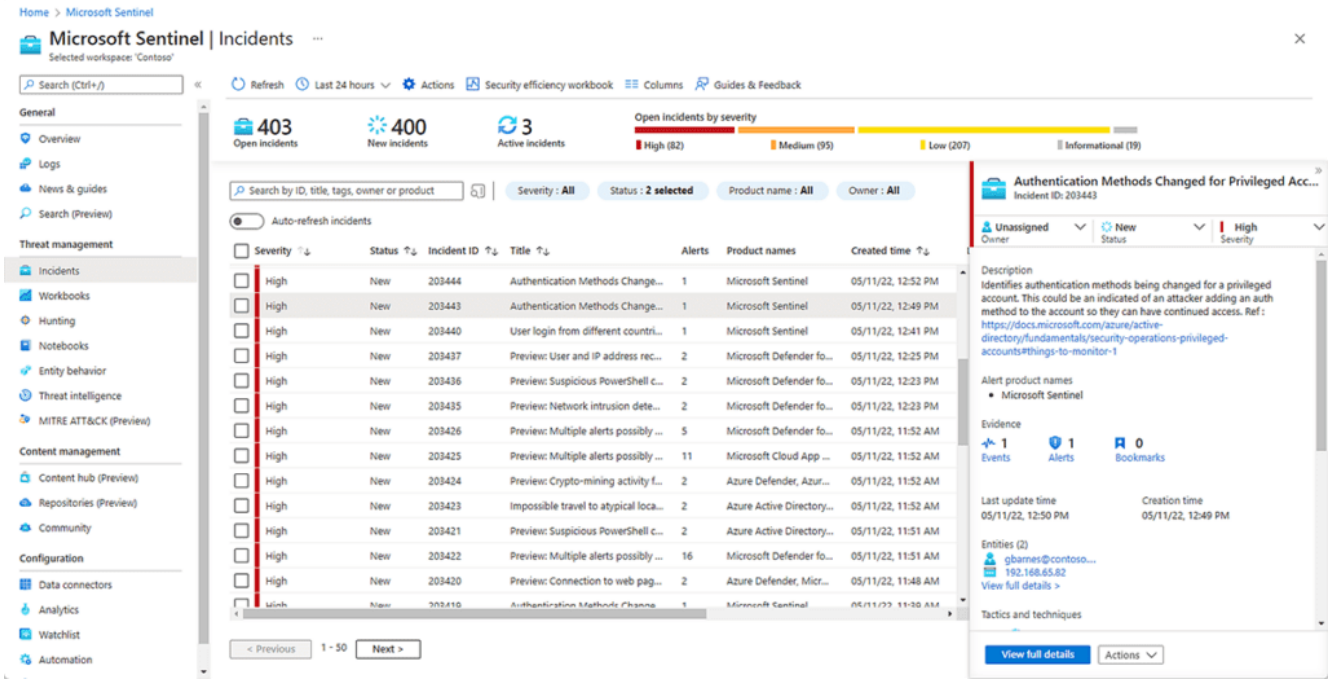

Рис. 1.9. Інтерфейс Microsoft Azure Sentinel

Однак, Azure Sentinel має кілька помітних недоліків. Вони використовують підхід до безпеки, що в першу чергу орієнтований на Microsoft, і не мають стільки ж інтеграцій зі сторонніми постачальниками рішень безпеки, як інші провідні SIEM-системи. Це робить їх непривабливим рішенням для організацій, які використовують продукти безпеки не від Microsoft. Також аналітикам безпеки, які не знайомі з джерелами даних Microsoft, доведеться досить складно навчитися [11].

Отже, оскільки кібератаки стають дедалі поширенішими та гучнішими, як ніколи важливо розуміти доступні інструменти кібербезпеки. Коли йдеться про звітність щодо безпеки, існує конфлікт між обсягом даних та практичністю. Хоча ми не хочемо пропустити жодної події безпеки, керувати всіма сповіщеннями від усіх систем вашої інфраструктури безпеки просто неможливо.

SIEM централізують всі сповіщення на одній платформі та сповіщають про будь-яку подію, яка потребує уваги, не витрачаючи час на моніторинг кількох систем. Щоб ще більше покращити свій профіль безпеки, ми можемо інтегрувати SIEM з такими рішеннями, як SOAR та UEBA, для автоматизації виявлення загроз, зменшення кількості хибнопозитивних результатів та реагування на загрози, або використовувати SIEM наступного покоління.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ І РЕАГУВАННЯ НА НИХ НА ОСНОВІ ПРАВИЛ FORTISIEM

2.1. Призначення та основні функції рішення FortiSIEM

FortiSIEM – це вдосконалене рішення для керування інформацією про безпеку та подіями (SIEM), яке поєднує розширений аналіз журналів і трафіку з моніторингом продуктивності/доступності, аналізом змін і точним знанням інфраструктури для забезпечення точного виявлення загроз, усунення проблем, реагування на інциденти та звітування про відповідність [8].

FortiSIEM можна розгорнути як апаратний пристрій, віртуальний пристрій або як кластер віртуальних пристроїв для масштабування до великих розгортань інфраструктури. FortiSIEM плавно масштабується від малих підприємств до великих і територіально розподілених підприємств і постачальників послуг [8].

Для невеликих розгортань FortiSIEM можна розгорнути як єдине апаратне забезпечення «все в одному» або віртуальний пристрій, який містить повну функціональність продукту. Віртуальний пристрій може працювати на більшості поширених гіпервізорів, включаючи VMware ESX, Microsoft Hyper-V і RedHat KVM, і може бути розгорнуто на місці або в Amazon AWS Cloud. Для великих середовищ, які потребують більшої пропускної здатності обробки подій і зберігання, FortiSIEM можна розгорнути в режимі кластера. Існує чотири типи вузлів FortiSIEM – Collector, Worker, Supervisor (Supervisor with Database, Supervisor Without Database) і Database Server. Вузли сервера бази даних можуть формувати кластер БД для підтримки масштабованого кластера Supervisor Without Database для забезпечення значно вищого рівня підтримки користувачів.

Колектори використовуються для масштабування збору даних із різних георозділених мережевих середовищ, потенційно за брандмауером. Збирачі спілкуються з пристроями, збирають дані, аналізують дані та надсилають їх до

робочих вузлів через стислий безпечний канал HTTP(s). Вузли Supervisor і Worker знаходяться в центрі обробки даних і виконують функції аналізу даних за допомогою розподілених кооперативних алгоритмів. Для масштабованого зберігання подій FortiSIEM надає три рішення: базу даних подій FortiSIEM NoSQL із даними, що зберігаються на сервері NFS, ClickHouse і Elasticsearch.

У міру зростання потреб у обчисленнях або сховищі можна додавати вузли Collector, робочі вузли, диски на сервері NFS, вузли даних ClickHouse і вузли даних Elasticsearch. FortiSIEM також надає агенти Windows, які дозволяють збирати журнали з великої кількості серверів Windows. Агенти Windows можна налаштувати для надсилання подій до збирачів у високодоступний спосіб збалансованого навантаження [8].

FortiSIEM дозволяє керувати декількома групами пристроїв і користувачів (організаціями) в рамках однієї інсталяції FortiSIEM. Пристрої та IP-адреси можуть збігатися між організаціями. FortiSIEM забезпечує суворе логічне розділення між організаціями на прикладному рівні. Користувачі однієї організації не можуть бачити дані іншої організації, включаючи пристрої, користувачів і журнали. Користувачі, які належать до організації керування постачальником послуг, можуть бачити всі організації.

Для повної обізнаності про ситуацію користувачеві необхідно глибоко знати мережеву та серверну інфраструктуру. Вбудований механізм виявлення FortiSIEM може досліджувати IT-інфраструктуру (локальну та хмарну, фізичну та віртуальну), глибоко виявляти та класифікувати мережеві пристрої, сервери, користувачів і програми. Виявляється широкий діапазон інформації, включаючи інформацію про обладнання, серійні номери та ліцензії, встановлене програмне забезпечення, запущені програми та служби, а також конфігурації пристроїв. Можна виявити деякі спеціальні топологічні зв’язки, наприклад, точки доступу WLAN до контролерів WLAN і гостьові системи VMware до фізичних хостів. Ця багата інформація заповнює інтегровану базу даних керування конфігураціями (CMDB), яка підтримується в актуальному стані шляхом запланованих повторних відкриттів [8].

Новим аспектом виявлення FortiSIEM є те, що система автоматично виявляє, що можна контролювати та який журнал можна витягти, використовуючи надані облікові дані. Цей підхід зменшує помилки людини, оскільки FortiSIEM автономно вивчає справжній стан конфігурації мережі.

FortiSIEM має гнучку розподілену архітектуру збору та аналізу журналів. Для журналів, переданих у FortiSIEM (наприклад, Syslog), пристрої можуть балансувати навантаження журналів між різними робочими або збирачами. Для журналів, отриманих за допомогою FortiSIEM (наприклад, Windows WMI або хмарних служб через REST API), функція отримання автоматично розподіляє навантаження між Worker і Collectors. Журнали негайно аналізуються в точці, де вони отримані. Ця розподілена обробка прискорює збір і аналіз журналів [8].

FortiSIEM має запатентовану мову синтаксичного аналізу журналів на основі XML, яка є одночасно гнучкою та ефективною з точки зору обчислень. Гнучкість полягає в тому, що користувачі можуть легко писати власні парсери (файли XML) або редагувати надані системою за допомогою графічного інтерфейсу FortiSIEM. XML-файли парсера компілюються під час виконання та виконуються як ефективний код. Це робить розбір журналів дуже ефективним, майже таким же ефективним, як написання коду рідними мовами програмування.

Шкідливе програмне забезпечення нульового дня може створювати проблеми з продуктивністю на сервері, наприклад, шкідливе програмне забезпечення може споживати великий обсяг пам’яті, або програмне забезпечення-вимагач сканування та шифрування файлів може сповільнити продуктивність інших програм. Закриваючи певні служби та створюючи надмірний мережевий трафік, зловмисне програмне забезпечення може спричинити проблеми з доступністю. Щоб належним чином виявити та усунути проблеми безпеки, досліднику необхідно знати тенденції продуктивності та доступності служб критичної інфраструктури. Завдяки своїм можливостям виявлення FortiSIEM може легко збирати різноманітні показники продуктивності та доступності, щоб допомогти досліднику шукати загрози. FortiSIEM також може сповіщати користувачів, коли він отримує показники за межами звичайного

профілю, співвідносячи такі порушення з проблемами безпеки для створення сповіщень високої точності.

Несанкціоновані або випадкові зміни ключових файлів конфігурації системи (наприклад, *httpd.conf*) або конфігурації маршрутизатора/брандмауера можуть призвести до проблем із безпекою. Шкідливе програмне забезпечення може змінювати ключові системні файли. Зловмисники (наприклад, інсайдерські загрози) можуть викрасти заборонені файли. Важливо підтримувати контроль над ключовими файлами та каталогами [8].

FortiSIEM надає механізми для відстеження та виявлення змін ключових файлів. Він може контролювати запуск і роботу мережевих пристроїв через SSH. Він може контролювати конфігураційні файли на серверах. Агенти FortiSIEM можуть ефективно контролювати великі серверні інфраструктури. Сповіщення створюється, коли файл змінюється з однієї версії на іншу або відхиляється від благословенної надійної конфігурації.

Хоча FortiSIEM забезпечує готову підтримку для великої кількості пристроїв і програм, користувачі можуть створювати власну повноцінну підтримку з графічного інтерфейсу користувача. Синтаксичні аналізатори системного журналу, монітори продуктивності та детектори зміни конфігурації можуть бути змінені. Можна визначити нові типи пристроїв і програм, монітори продуктивності та детектори змін конфігурації, а також інтегрувати нові парсери журналів для роботи з FortiSIEM.

Поєднуючи журнали DHCP, журнали VPN, журнали WLAN і події входу в систему контролера домену, FortiSIEM може підтримувати контрольний журнал для відображення IP-адреси користувача та географічного розташування протягом певного часу. Хоча зіставлення IP-адреси з користувачем є важливим для цілей пошуку, ця функція дозволяє FortiSIEM виявляти вкрадені облікові дані, оскільки вони мають тенденцію використовуватися з віддалених місць протягом короткого періоду часу.

Зовнішні веб-сайти можуть надавати інформацію про кіберзагрози з точки зору [8]:

шкідливе програмне забезпечення IP;

домен шкідливих програм;

хеш шкідливого програмного забезпечення;

URL-адреса шкідливого програмного забезпечення;

анонімізовані мережі.

FortiSIEM має гнучку структуру для підключення до широкого спектру джерел загроз (як безкоштовних, так і платних), ефективного завантаження цієї інформації та пошуку збігів у реальному часі в середовищі, у якому він працює. Деякі джерела загроз можуть мати велику кількість (мільйони) неправильних IP-адрес і URL-адрес. Механізми розподіленого пошуку та правил FortiSIEM знаходять збіги з такими великими наборами даних із дуже високою частотою подій.

Коли спрацьовує правило кореляції, у FortiSIEM створюється інцидент (рисунок 2.1).

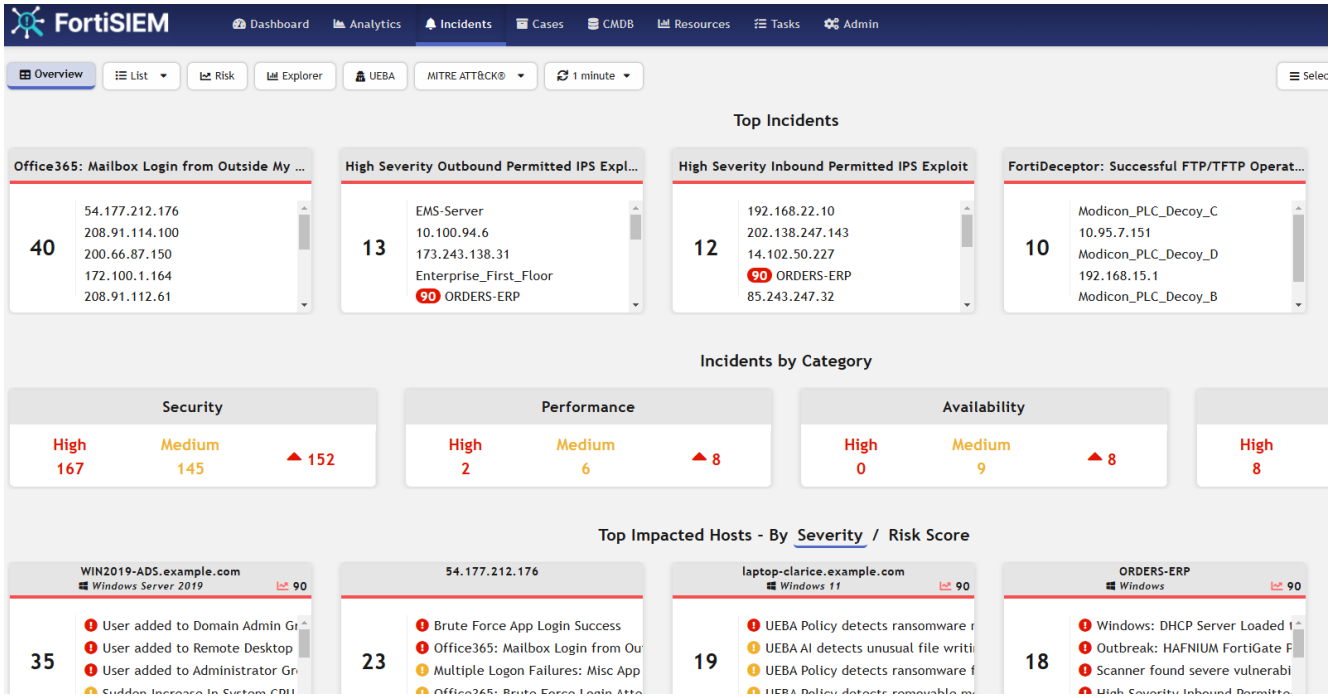

Рис. 2.1. Вкладка дослідження інцидентів безпеки

Поєднуючи критичність активів, роль і важливість користувача, серйозність інциденту, частоту виникнення та знайдені вразливості, FortiSIEM призначає

оцінку ризику користувачам і машинам. Ця оцінка відображається на інформаційній панелі з можливостями деталізації для визначення факторів, що лежать в основі.

FortiSIEM надає низку сценаріїв пом’якшення, які можуть виконувати дії, коли трапляється інцидент. Сценарії можуть бути викликані автоматично, коли відбувається інцидент, або можуть бути викликані на вимогу. Деякі приклади включають блокування IP або MAC адрес, дезактивацію користувача з активного каталогу, видалення зараженого файлу, додавання користувача до списку спостереження, перезапуск процесу або перезавантаження сервера тощо. Користувачі даної системи також можуть написати власні сценарії пом’якшення та розгорнути їх у працюючій системі.

FortiSIEM надає гнучку та уніфіковану систему пошуку. Користувач може шукати дані за ключовими словами або структуровано за допомогою аналізованих атрибутів FortiSIEM. У режимі реального часу відображаються відповідні дані, що надходять із пристроїв. В історичному режимі здійснюється пошук подій у базі даних подій. Вузли Supervisor і Worker виконують пошук розподіленим способом.

Надається велика кількість вбудованих звітів (шаблони пошуку) на основі типу пристрою та функціональних можливостей, таких як доступність, продуктивність, зміни та безпека.

Двома новими аспектами пошуку FortiSIEM є уніфікація подій і можливості деталізації або пошуку загроз. За допомогою об’єднання подій усі дані аналізуються та подаються однаково, будь то аспекти презентації (пошук у реальному часі, звіти, правила) або контекст (показники продуктивності та доступності, події змін чи журнали безпеки). За допомогою деталізації пошук можна розпочати з певного контексту, як-от «Найпоширеніші користувачі, які не пройшли автентифікацію», і вибрати атрибути для подальшого аналізу даних і ітеративного пошуку основної причини проблеми. Як приклад, розслідування «найчастіших користувачів із помилками автентифікації» може супроводжуватися вибором певного користувача зі списку та вибором IP-адреси призначення та

портів, щоб побачити, з якими машинами спілкувався користувач, а потім вибирати необроблені журнали для реальних доказів.

FortiSIEM містить широкий вибір готових звітів про відповідність – PCI, COBIT, SOX, ISO, ISO 27001, HIPAA, GLBA, FISMA, NERC, GPG13, SANS Critical Control, NIST800-53 і NIST800-171.

FortiSIEM надає широкий вибір візуальних панелей для даних, які він збирає, і для інцидентів, які викликали: панелі підсумків, панелі віджетів, панель бізнес-служб, панель інцидентів і панель ідентифікації та місцезнаходження.

FortiSIEM має вбудовану систему тикетів для керування інцидентами за допомогою тикетів. Рішення підтримує повний життєвий цикл заявки: відкриття, ескалація, закриття, повторне відкриття та створення справ із вкладеннями для доказів.

FortiSIEM забезпечує аналітику бізнес-послуг. Business Service дозволяє визначати пріоритети інцидентів і переглядати показники продуктивності/доступності з точки зору бізнес-послуг. Business Service визначається у FortiSIEM як інтелектуальний контейнер відповідних пристроїв і програм, які служать загальним бізнес-цілям. Після визначення весь моніторинг і аналіз представлені з точки зору бізнес-послуг.

FortiSIEM дозволяє легко визначати та підтримувати Business Service. Оскільки FortiSIEM автоматично виявляє програми, запущені на серверах, а також підключення до мережі та потік трафіку, ми можемо легко вибрати програми та відповідні сервери та отримувати інтелектуальні підказки щодо вибору решти компонентів Business Service.

2.2. Архітектура рішення FortiSIEM та основні процеси функціонування

Рішення FortiSIEM можна плавно масштабувати від малих підприємств до великих і територіально розподілених підприємств і постачальників послуг.

Для невеликих розгортань FortiSIEM можна розгорнути як єдине апаратне

забезпечення «все в одному» або віртуальний пристрій, який містить повну функціональність продукту. У FortiSIEM це вузол Supervisor.

Для великих середовищ, які потребують більшої пропускної здатності обробки подій, FortiSIEM можна розгорнути в кластері віртуальних пристроїв Supervisor і Worker. Вузли колектора також використовуються для розподілу збору подій між колекторами з метою підвищення продуктивності та архітектури, наприклад збору подій із віддалених мереж і різних сегментів мережі.

Для великих розподілених середовищ, де є кілька екземплярів FortiSIEM, FortiSIEM Manager можна використовувати для моніторингу окремих екземплярів FortiSIEM і керування інцидентами. FortiSIEM Manager є окремим ліцензованим продуктом FortiSIEM. Якщо немає потреби керувати декількома екземплярами FortiSIEM (супервізорами), встановлюється єдиний Supervisor, який керуватиме робочими вузлами, вузлами колектора та агентами.

Існує чотири типи вузлів FortiSIEM – Collector, Worker, Supervisor і Manager. Колектори використовуються для масштабування збору даних із різних територіально відокремлених мережевих середовищ, потенційно за брандмауерами. Колектори спілкуються з пристроями, збирають, аналізують і стискають дані, а потім надсилають цю інформацію робочим вузлам через захищений канал HTTP(s) із збалансованим навантаженням. Вузли Supervisor і Worker знаходяться в центрі обробки даних і виконують функції аналізу даних за допомогою розподілених кооперативних алгоритмів.

Екземпляр FortiSIEM складається з Supervisor, кількох Workers і Collectors. FortiSIEM Manager можна використовувати для моніторингу та керування кількома екземплярами FortiSIEM через канал HTTPs REST API. Відомості про інциденти, ліцензію та стан справ пересилаються з кожного екземпляра FortiSIEM до FortiSIEM Manager. У FortiSIEM Manager можна очистити/вирішити/змінити серйозність/додати коментарі до одного чи кількох інцидентів, вимкнути одне чи кілька правил і змінити їх серйозність, запустити FortiSOAR Playbooks і конектори для оновлення статусу інциденту та коментарів. Операція одним натисканням для входу у відповідний екземпляр FortiSIEM, де стався інцидент.

Це дає змогу швидко детально розслідувати інцидент.

FortiSIEM – це гнучке рішення, яке можна розгортати різними способами для задоволення різних вимог до продуктивності, масштабованості та топології. Основними сценаріями розгортання є малий і середній бізнес (SMB), підприємство та постачальник послуг [9].

Необхідно відмітити, що розгортання для SMB зазвичай менші та можуть складатися з комплексного або невеликого розподіленого рішення (рисунок 2.2).

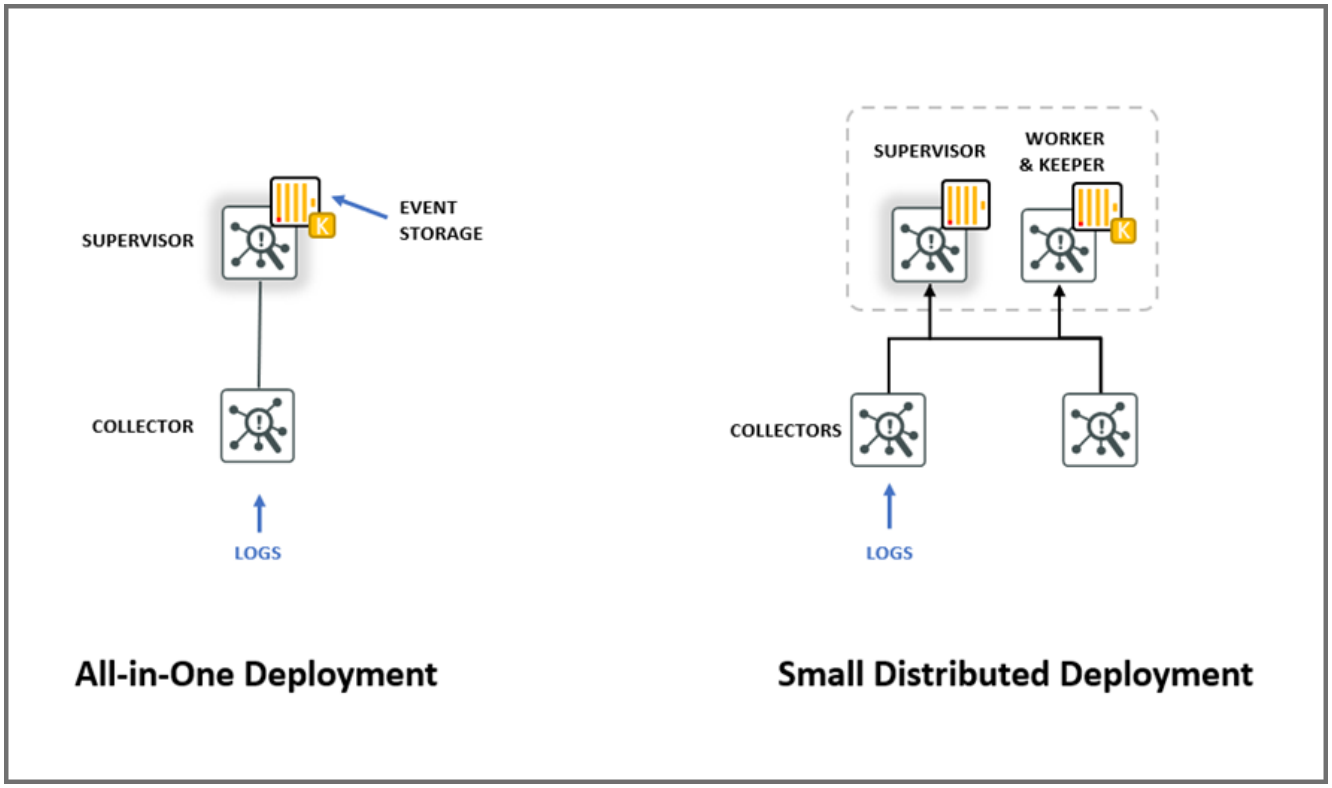

Рис. 2.2. Архітектура рішення FortiSIEM для SMB [9]

Універсальна архітектура FortiSIEM – це легке в розгортанні автономне єдине серверне рішення, яке підходить для невеликих розгортань. У цій архітектурі розгорнуто лише вузол FortiSIEM Supervisor. Він запускає графічний інтерфейс користувача, додаток FortiSIEM, базу даних ClickHouse з єдиним сегментом і без реплік, а також процеси зберігача ClickHouse.

Підприємства малого та середнього бізнесу, яким потрібна додаткова масштабованість для задоволення поточних або майбутніх вимог до потужності та продуктивності, повинні використовувати невелике розподілене рішення з вузлом

Supervisor і Worker. Невеликі додаткові витрати додаткового вузла забезпечують значні переваги, а саме система є значно більш масштабованою. Також підвищується стійкість завдяки тому, що Worker розміщує другу репліку [9].

Колектори можна використовувати з обома архітектурами для віддаленого збору журналів сайту, для розвантаження збору журналів і моніторингу продуктивності з супервізора, а також для збору журналів агента. Організаціям слід запланувати розгортання принаймні одного Collector для допомоги у зборі журналів і для підтримки агентів сервера FortiSIEM.

Є п’ять основних завдань аналізу даних [8]:

індексація даних та зберігання в базі даних подій;

пошук даних;

кореляція даних у потоковому режимі для запуску правил (аномалії поведінки);

створення бази даних ідентифікації користувача та розташування для додавання контексту для даних;

створення базових ліній для виявлення аномалій.

Для масштабованості кожне з цих завдань розділено на важкий робочий компонент, який виконується робочими вузлами, і легкий головний компонент, який виконується вузлом Supervisor. *Вузли Supervisor, доступні через графічний інтерфейс, складаються з автономної трирівневої моделі – графічного інтерфейсу користувача, сервера додатків, що містить бізнес-логіку, і реляційної бази даних для збереження стану програми FortiSIEM.*

Для масштабованого зберігання подій FortiSIEM пропонує три варіанти [8]:

локальний диск – база даних подій FortiSIEM NoSQL із даними, що зберігаються на сервері NFS;

розподілена база даних Elasticsearch – апаратні пристрої та універсальні рішення для віртуальних пристроїв використовують опцію локального диска, тоді як опції NoSQL або Elasticsearch можуть бути використані кластером FortiSIEM Supervisor і Workers;

база даних подій NoSQL – це спеціально створене власне рішення

FortiSIEM. Вузли Supervisor і Worker створюють і підтримують індекси бази даних. Для масштабування продуктивності вставки подій і пошуку в цьому режимі потрібні:

швидка мережа зв’язку між вузлами Supervisor/Worker і сервером NFS;

високий IOPS NFS, якого можна досягти за допомогою швидкого диска RAID або багаторівневого SSD і магнітних дисків.

Elasticsearch забезпечує справжню розподілену надлишкову базу даних у вигляді стовпців для масштабування продуктивності бази даних за рахунок вищих потреб у сховищі. У цьому варіанті вузли FortiSIEM Worker надсилають дані в реальному часі до кластера Elasticsearch, який підтримує базу даних подій. FortiSIEM розробив проміжний рівень адаптації, щоб той самий графічний інтерфейс міг безперебійно працювати як у Elasticsearch, так і в базі даних подій FortiSIEM NoSQL.

2.3. Призначення та види правил в системі FortiSIEM

Кореляція розподілених подій і виявлення загроз системою FortiSIEM здійснюється механізмом правил.

Система FortiSIEM має механізм розподіленої кореляції подій, який може виявляти складні загрози майже в реальному часі. Загрози – це аномалії поведінки користувачів або комп’ютерів, які можна вказати за допомогою шаблонів подій, упорядкованих у часі. Загрозу можна альтернативно розглядати як SQL-запит, оцінений у потоковому режимі. FortiSIEM має вбудований механізм профілювання, який може обробляти загрози, визначені за допомогою статистичних порогів, використовуючи середнє значення та стандартне відхилення [8].

Що робить систему правил FortiSIEM потужною, так це [8]:

можливість включати будь-які дані в правило, наприклад: продуктивність і показники змін разом із журналами безпеки, (б) розподілені обчислення в пам’яті (заявка на патент) із залученням вузлів Supervisor і Worker для продуктивності

майже в реальному часі з високою частотою подій;

здатність правила генерувати динамічний список спостереження, який можна рекурсивно використовувати в новому правилі для створення вкладена ієрархія правил;

використання об’єктів CMDB у визначенні правила;

уніфікована мова на основі XML для правил і звітів, що дозволяє легко перетворювати звіт у правило і навпаки.

Кілька моделей UEBA на основі машинного навчання є частиною вбудованої бібліотеки правил FortiSIEM [8]:

виявлення одночасних входів із двох різних країн;

виявлення одночасних входів із двох малоймовірних геолокацій;

аномалія поведінки входу – вхід на сервери в той час, коли користувач зазвичай не входить, тощо;

виявлення трафіку до динамічно генерованих доменів.

FortiSIEM має велику кількість вбудованих правил поведінкових аномалій, які працюють із коробки, але також можуть бути адаптовані користувачем для власного середовища. Надається структура, де користувач може писати нові правила за допомогою графічного інтерфейсу користувача, перевіряти їх на реальних подіях, а потім розгортати в системі.

Система FortiSIEM постійно відстежує корпоративну IT-інфраструктуру та надає інформацію для аналізу продуктивності, доступності та безпеки. Також можуть виникати ситуації, коли нам потрібно отримувати сповіщення, коли виникають виняткові, підозрілі або потенційні умови збою. Ми можемо досягти цього за допомогою правил, які визначають умови, на які слід звернути увагу, і які викликають інцидент, коли ці умови виникають.

Ми можемо налаштувати політику автоматизації, яка надсилатиме сповіщення електронною поштою та SNMP про те, що стався інцидент. FortiSIEM включає понад 500 визначених системою правил, які можна переглянути в *RESOURCES > Rules*.

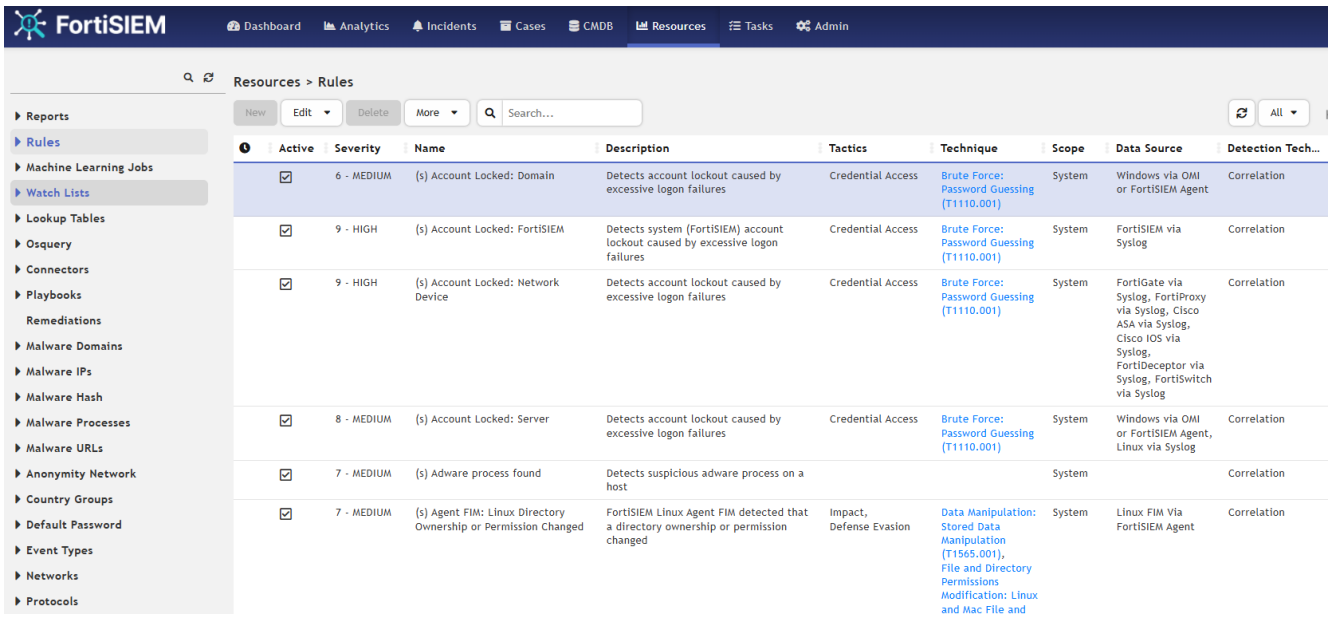

Рис. 2.7. Вкладка *Rules* [9]

Правила виявляють погані поведінкові аномалії для машин і користувачів у реальному часі. FortiSIEM розробив SQL-подібну мову специфікації правил на основі XML. Користувач створює правило з графічного інтерфейсу користувача, перевіряє його за допомогою реальних подій, а потім розгортає правило . Мова XML є досить потужною та використовує об’єкти CMDB (наприклад, групи пристроїв, мережі та програм, групи типів подій, об’єкти шкідливого програмного забезпечення, групи країн, списки спостереження), щоб зберегти правила лаконічними [8].

Специфікація правила включає кілька підшаблонів подій, з’єднаних логічними операторами (AND, OR, AND NOT, FOLLOWED BY і NOT FOLLOWED BY). Кожен підшаблон схожий на запит SQL із фільтрами, групуванням за атрибутами та пороговими значеннями для агрегатів. Порогові значення можуть бути статичними або динамічно визначеними на основі статистики. Правило може бути вкладеним, тобто правило може бути налаштовано для ініціювання іншого правила. Правило також може створити список спостереження, який, як і об’єкт CMDB, можна використовувати в іншому правилі [8].

Обчислення правил відбувається в потоковому режимі з використанням

розподілених обчислень у пам’яті за участю вузлів Super і Worker. Останні визначення правил поширюються на вузли Super і Worker. Робочі вузли оцінюють кожне правило на основі подій, які воно бачить, і періодично надсилають часткові результати правил до вузла Supervisor. Вузол Supervisor зберігає механізм станів глобального правила та створює інцидент, коли умови правила виконуються. Якщо правило містить статистичний атрибут (наприклад, середнє або стандартне відхилення), створюється базовий звіт, який обчислює статистичні дані та оновлює умови правила. Базовий звіт також виконується в потоковому режимі з використанням вбудованих розподілених обчислень. Коли об’єкт CMDB змінюється, модуль App Server на вузлі Supervisor надсилає сигнал про зміну робочим вузлам, які потім завантажують зміни. Це розподілене обчислення в пам’яті дозволяє FortiSIEM масштабувати продуктивність майже в реальному часі з високим EPS і великою кількістю правил [8].

Оскільки FortiSIEM аналізує всі дані, включаючи журнали, показники продуктивності та доступності, потоки та зміни конфігурації, механізм правил може виявити підозрілу поведінку. Ця здатність перехресної кореляції між різними функціональними доменами IT робить структуру правил FortiSIEM потужною та ефективною [8].

3. РЕКОМЕНДАЦІЇ ЩОДО ВИЯВЛЕННЯ ЗАГРОЗ КОРПОРАТИВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ І РЕАГУВАННЯ НА НИХ НА ОСНОВІ ПРАВИЛ FORTISIEM

3.1. Порядок створення правил рішення FortiSIEM для виявлення загроз корпоративним інформаційним ресурсам

Необхідно зазначити, що система FortiSIEM постійно відстежує корпоративну IT-інфраструктуру та надає інформацію для аналізу продуктивності, доступності та безпеки. Також можуть виникати ситуації, коли існує потреба отримувати сповіщення, коли виникають виняткові, підозрілі або потенційні умови збою.

Цього можна досягти за допомогою правил, які визначають умови, на які слід звернути увагу, і які викликають інцидент, коли ці умови виникають. Ми можемо налаштувати політику автоматизації, яка надсилатиме сповіщення електронною поштою та SNMP про те, що стався інцидент. FortiSIEM включає понад 500 визначених системою правил, які можна переглянути в *RESOURCES* > *Rules*, але ми також можемо створити власні правила.

FortiSIEM містить великий набір правил для груп *Availability, Performance, Change, Security* та *Beaconing* на додаток до правил, які ми можемо визначити для своєї системи.

Розглянемо порядок створення кореляційних правил в системі FortiSIEM.

Створення нового правила передбачає визначення атрибутів інциденту, який запускається правилом, а також умов запуску та будь-яких винятків або чітких умов. Можна створити правило, клонувавши існуюче правило за допомогою кнопки *Clone* та відредагувавши його.

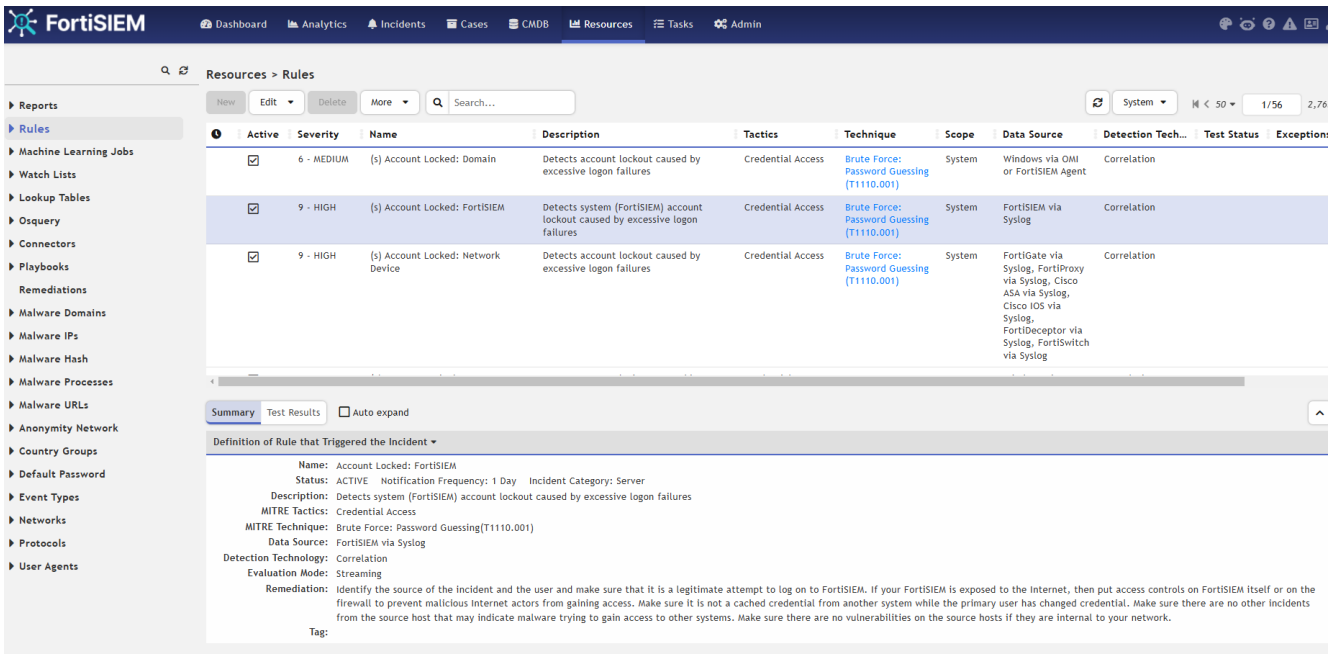

Рис. 3.1. Панель *Rules*

Щоб створити правило, виконайте наведені нижче дії.

1. Перейдіть до *RESOURCES* > *Rules*.

2. Виберіть групу, до якої потрібно додати нове правило.

3. Натисніть *New*, щоб створити нове правило.

При створенні нового правила необхідно вказати спосіб технології виявлення, який використовується цим правилом, вибравши зі спадного списку. Можливі варіанти:

кореляція – використовує зв’язок між змінними для відкриття;

кореляція за допомогою таблиці пошуку – використовує таблицю пошуку для виявлення;

машинне навчання – використовує моделі машинного навчання для виявлення;

профілювання – збирає певні дані для виявлення.

Необхідно налаштувати режим оцінювання. Для цього вибираємо *Streaming* або *Scheduled*. Правила потокового передавання – це правила, які виконуються в реальному часі. Заплановані правила – це правила, які виконуються за визначеним розкладом. Правила в режимі за розкладом вимагають налаштування вікна часу запиту та розкладу.

Також необхідно визначити дії правила. Зокрема, необхідно вибрати рівень серйозності, щоб пов’язати його з інцидентом, викликаним правилом. Необхідно вибрати категорію інцидентів, які будуть ініційовані правилом.

4. Натисніть *Save*.

Нове правило буде збережено у вибраній групі в неактивному стані. Перш ніж активувати правило, його слід перевірити.

Важливим моментом є визначення умов правила. Умови правила визначають атрибути події та порогові значення, які ініціюють інцидент. Умови правила складаються з підшаблонів фільтрів атрибутів подій і функцій агрегації. Ми можемо вказати більше одного підшаблону, а також зв’язки та обмеження між ними.

Підшаблон визначає характеристики подій, які призведуть до того, що правило запустить інцидент. Підшаблон передбачає визначення атрибутів подій, які будуть відстежуватися, а потім визначення порогових значень для агрегацій атрибутів подій, які ініціюють інцидент.

Для запланованих правил для середовищ, які не належать до ClickHouse, дозволено лише один підшаблон. Для середовищ ClickHouse заплановане правило може використовувати функції FOLLOWED_BY і NOT_FOLLOWED_BY для підшаблонів, додавши галочку до прапорця *Multiple Subpatterns*.

Умови агрегування груп встановлюють поріг, за якого певна агрегація подій запускатиме правило для створення інциденту. Ми створюємо умову агрегування за допомогою конструктора виразів, щоб налаштувати функцію, а потім вводимо оператор і значення для умови агрегування. В таблиці 3.1 наведено приклади налаштувань групування та сукупних умов.

Якщо у нас є більше одного підшаблону, ми повинні вказати зв’язок між ними за допомогою операторів, наведених в таблиці 3.2.

Ми можемо зв’язати атрибути підшаблону з відповідними атрибутами іншого підшаблону у спосіб, подібний до операції JOIN у SQL, за допомогою операторів зв’язку < , > , <= , >= , = , != . Приклади зв’язків і обмежень між підшаблонами наведено у таблиці 3.3.

Таблиця 3.1

Приклади налаштувань групування та сукупних умов

Scenario	Group By Attributes	Aggregate Conditions
10 or more events	none	**COUNT(Matched events) >= 10**
Connections to 100 or more distinct destination IPs from the same source IP	**Source IP**	**COUNT (DISTINCT Destination IP) >= 100**
Connections to 100 or more distinct destination IPs from the same source IP on the same destination port	**Source IP,Destination Port**	**COUNT (DISTINCT destination IP) >= 100**
Average CPU Utilization on the same server > 95% over 3 samples	**Host IP**	**COUNT (Matched Events) >= 3 AND AVG(CPU Util) > 95**
Logins from the same source workstation to 5 or more accounts on the same target server	**Source IP**, **Destination IP**	**COUNT(DISTINCT user) >= 5**

Таблиця 3.2

Оператори для систем підшаблонів

Operator	Meaning
AND	**Sub-pattern P1 AND Sub-pattern P2** means both sub-patterns P1 and P2 have to occur
OR	**Sub-pattern P1 OR Sub-pattern P2** means either P1 or P2 have to occur
FOLLOWED-BY	**Sub-pattern P1 FOLLOWED-BY Sub-pattern P2** means P1 has to be followed by P2 in time
AND-NOT	**Sub-pattern P1 AND-NOT Sub-pattern P2** means P1 must occur while P2 must not; the time order between P1 and P2 is not important
NOT-FOLLOWED-BY	**Sub-pattern P1 NOT-FOLLOWED-BY P2** means P1 must occur and P2 must not occur after P1

Таблиця 3.3

Приклади зв’язків і обмежень між підшаблонами

Scenario	Sub-pattern P1 - filter	P1 - Group-by attribute set	P1 Group constraint	Sub-pattern P2 filter	P2-group-by attribute	P2 group constraint	Inter-P1-P2 relationships	Inter-P1-P2 constraints
5 login failures from the same source to a server not followed by a successful logon from the same source to the same server	Event type = Login Success	Source IP, Destination IP	COUNT (Matched Event) >= 5	Event type = Login failure	Source IP, Destination IP	COUNT(Matched Event) > 0	P1 NOT_FOLLOWED_BY P2	P1's Source IP = P2's Source IP
An security attack to a server followed by the server scanning the network, that is, attempting to communicate to 100 distinct destination IP addresses in 5 minute time windows	Event type = Attack	Destination IP	COUNT (Matched Event) > 0	Event Type = Connection Attempted	Source IP	COUNT (DISTINCT Destination IP) > 100	P1 FOLLOWED_BY P2	P1's Destination IP = P2's Source IP
Average CPU > 95% over 3 sample on a server AND Ping loss > 75%	Event Type = CPU_Stat	Host IP	COUNT(Matched Event) >= 3 AND AVG(cpuUtil) > 95	Event Type = PING Stat	Host IP	pingLossPct > 75	P1 AND P2	P1's Host IP = P2's Host IP

Визначення інциденту, створеного правилом, передбачає встановлення атрибутів для інциденту на основі підшаблонів, які ми створили як умови для правила, а потім встановлення атрибутів для інциденту, які використовуватимуться в аналітиці та звітах.

Після активації правила воно постійно відстежує корпоративну IT-інфраструктуру на наявність умов, які можуть викликати подію. Однак ми також можете визначити винятки з цих умов. Наприклад, ми можемо знати, що сервер буде вимкнено на технічне обслуговування протягом певного періоду часу, і ми не хочемо, щоб наше правило «Server Down – No Ping Response» викликало інцидент для нього.

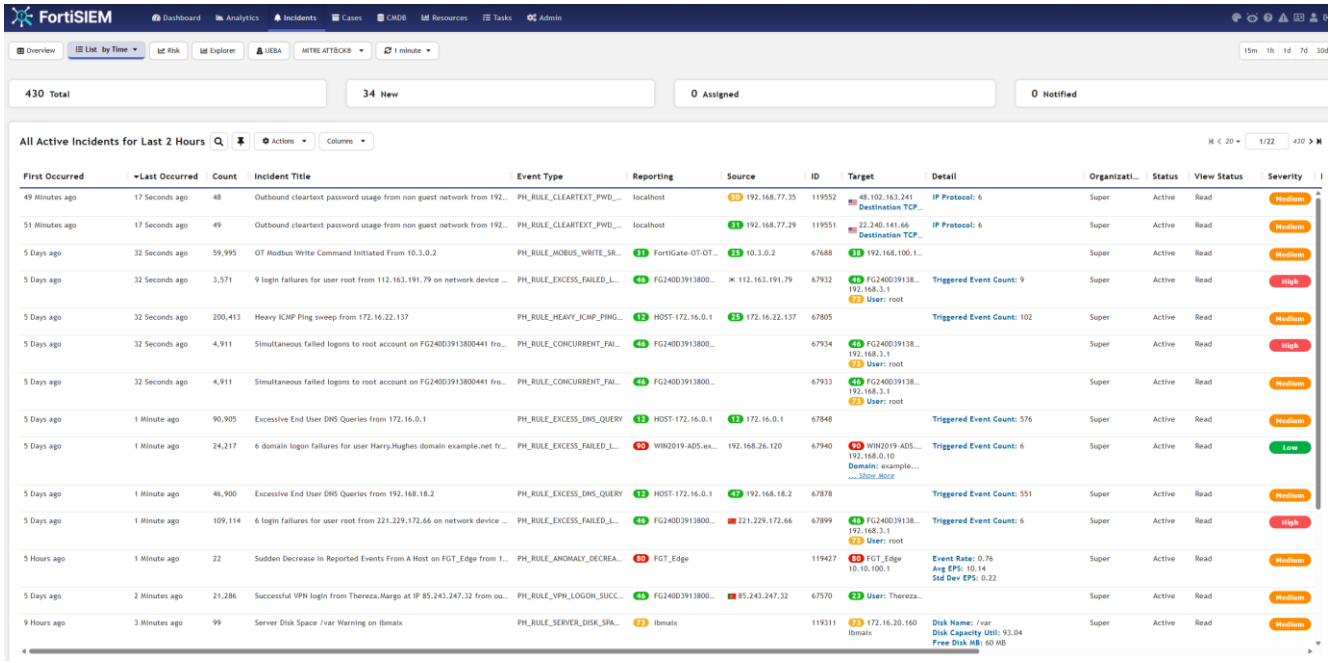

Рис. 3.2. Назви інцидентів в таблиці списку інцидентів

При очищенні умов визначаються умови, за яких статус інцидентів буде змінено з «Активний» на «Вирішено». Ми можемо встановити період часу, який має пройти, щоб виникла умова очищення, а потім встановити умови на основі запуску початкового правила або на основі підшаблону на основі атрибутів інциденту.

Визначення назви інциденту полегшує ідентифікацію інциденту без

необхідності шукати джерело, ціль і подробиці інциденту. Ми можемо визначити заголовки як для визначених користувачем, так і для системних правил.

У цих кроках передбачається, що ми вже створили правило або редагуємо системне правило.

Після створення або редагування правила ми повинні перевірити його, щоб побачити, чи воно працює належним чином, перш ніж активувати.

3.2. Порядок роботи з інцидентами в середовищі рішення FortiSIEM

Коли спрацьовує правило кореляції, у FortiSIEM створюється інцидент.

Перегляд «*Overview*» забезпечує перегляд «згори вниз» різних типів інцидентів і постраждалих хостів. Для цього необхідно перейти до *INCIDENTS* > *Overview*, щоб переглянути це подання.

Панель розділена на три секції (рисунок 3.3):

Incidents by Category – відображає кількість інцидентів за функціями та серйозністю;

Top Incidents – відображає найпопулярніші інциденти, відсортовані спочатку за серйозністю, а потім за кількістю;

Top Impacted Hosts – відображає найбільш постраждалі хости за ступенем серйозності або ризику.

У режимі перегляду *Risk* (рисунок 3.4) відображаються сутності (пристрої та користувачі), упорядковані за ризиком. Ризик розраховується на основі інцидентів, що викликають інциденти, за допомогою власного алгоритму, який включає критичність активів, серйозність інцидентів, частоту виникнення інцидентів і знайдені вразливості. Ризик обчислюється лише для пристроїв у CMDB, приватних IP-адрес і користувачів, знайдених у журналах або виявлених через LDAP.

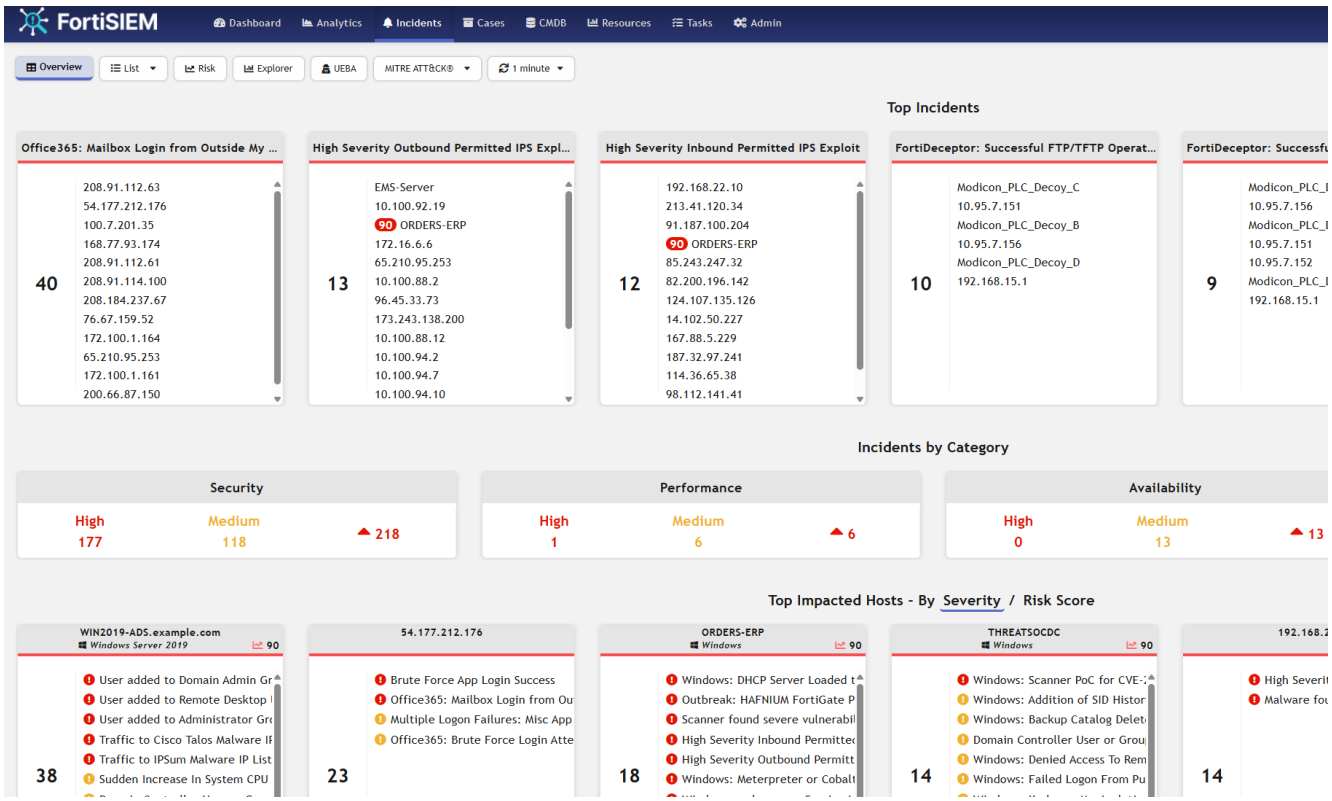

Рис. 3.3. Вкладка *Overview*

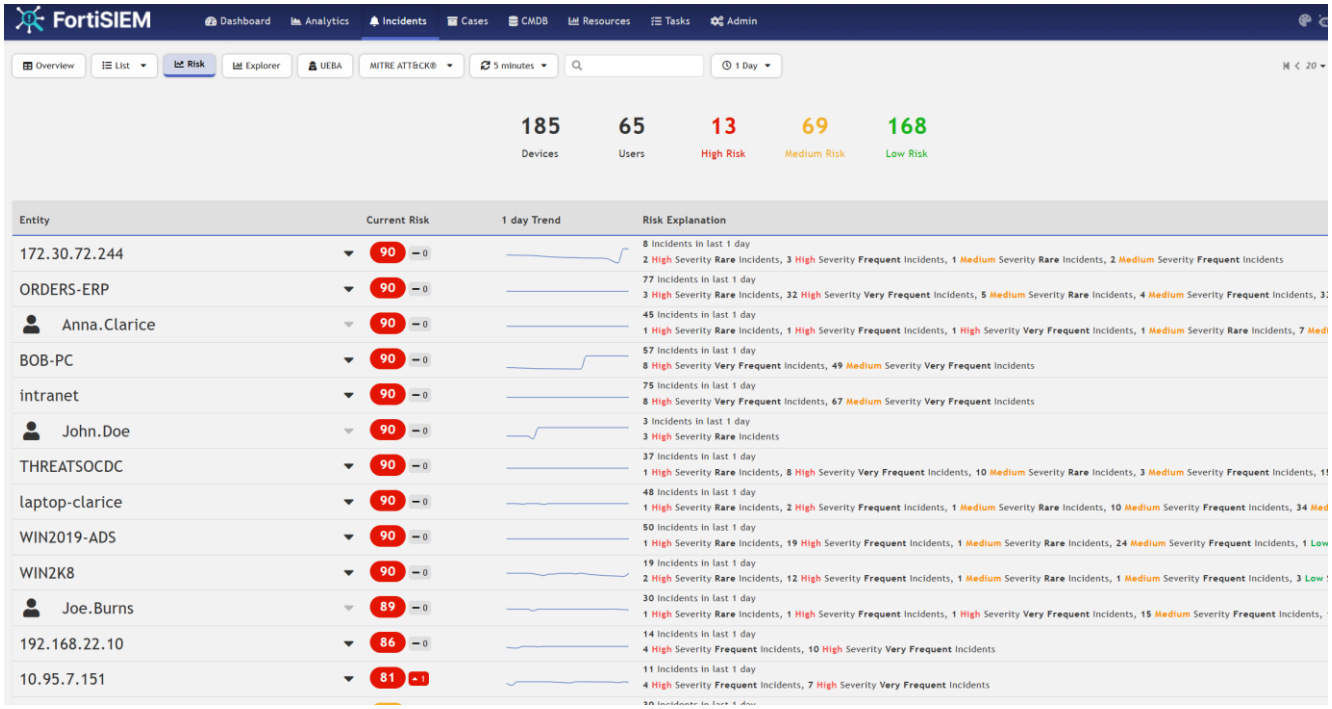

Рис. 3.4. Вкладка *Risk*

Пристрої та користувачі класифікуються за ризиком таким чином:

пристрої – кількість пристроїв із ризиком;

користувачі – кількість користувачів із ризиком;

високий ризик – кількість пристроїв і користувачів із високим ризиком;

середній ризик – кількість пристроїв і користувачів із середнім ризиком;

низький ризик – кількість пристроїв і користувачів із низьким ризиком.

Перегляд ризиків відображає наступне:

сутність (пристрій або ім’я користувача);

параметри деталей сутності (для пристроїв доступні дії зі спадним меню);

поточний ризик – поточне значення, підвищення або зниження порівняно з тим самим періодом;

тенденція ризику за 24 години (тенденція за 1 день);

інциденти за останні 24 години (1 день).

Перегляд Incident Explorer (рисунок 3.5) дозволяє співвідносити учасників (IP, хост, користувач) між кількома інцидентами без створення кількох звітів на окремих вкладках. Тенденції інцидентів, актора та деталі інциденту відображаються на одній сторінці. Ми можемо вибрати актора та побачити всі події, у яких цей актор бере участь.

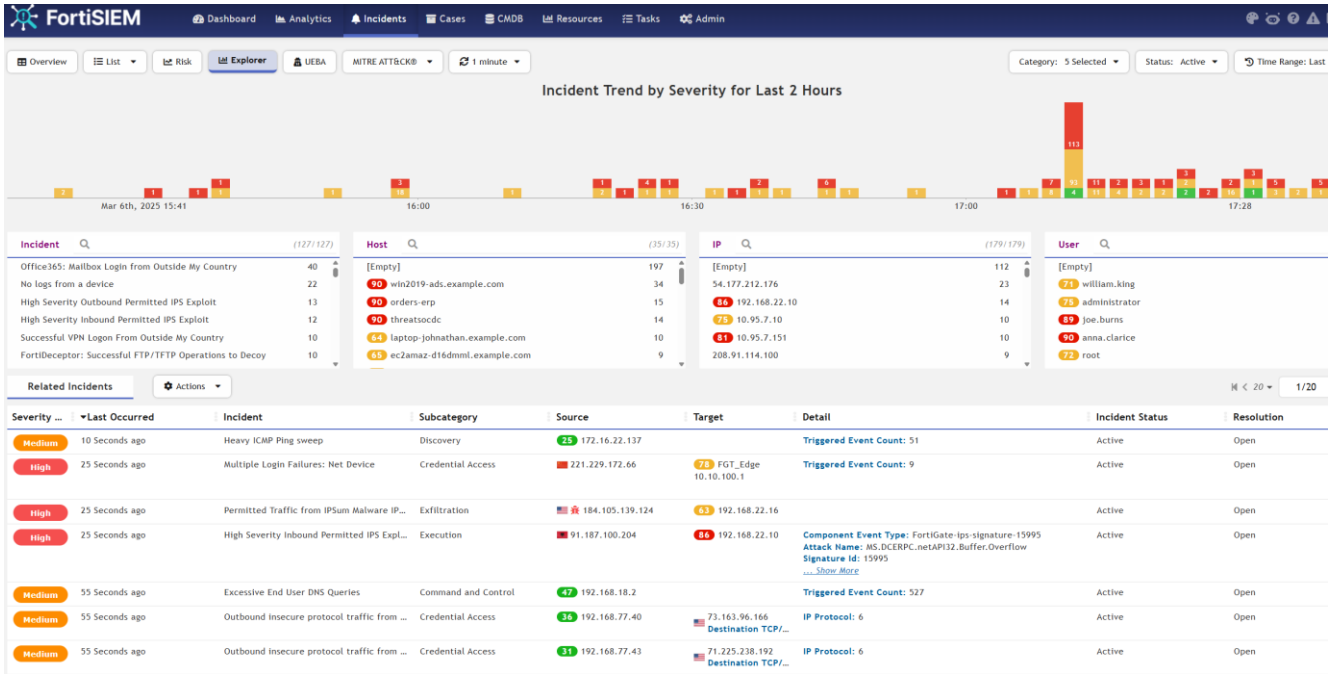

Рис. 3.5. Вкладка *Explorer*

Потім ми можемо вибрати часовий діапазон і звузити коло подій. Діапазони часу, актори та інциденти можна вибирати в будь-якому порядку. Щоразу, коли робиться вибір, решта інформаційної панелі оновлюється відповідно до цього вибору.

Перегляд UEBA відстежує сповіщення AI, отримані від FortiInsight. Перегляд UEBA розділений на такі рівні (рисунок 3.6):

графік тенденцій інцидентів;

список атрибутів;

пов’язані інциденти.

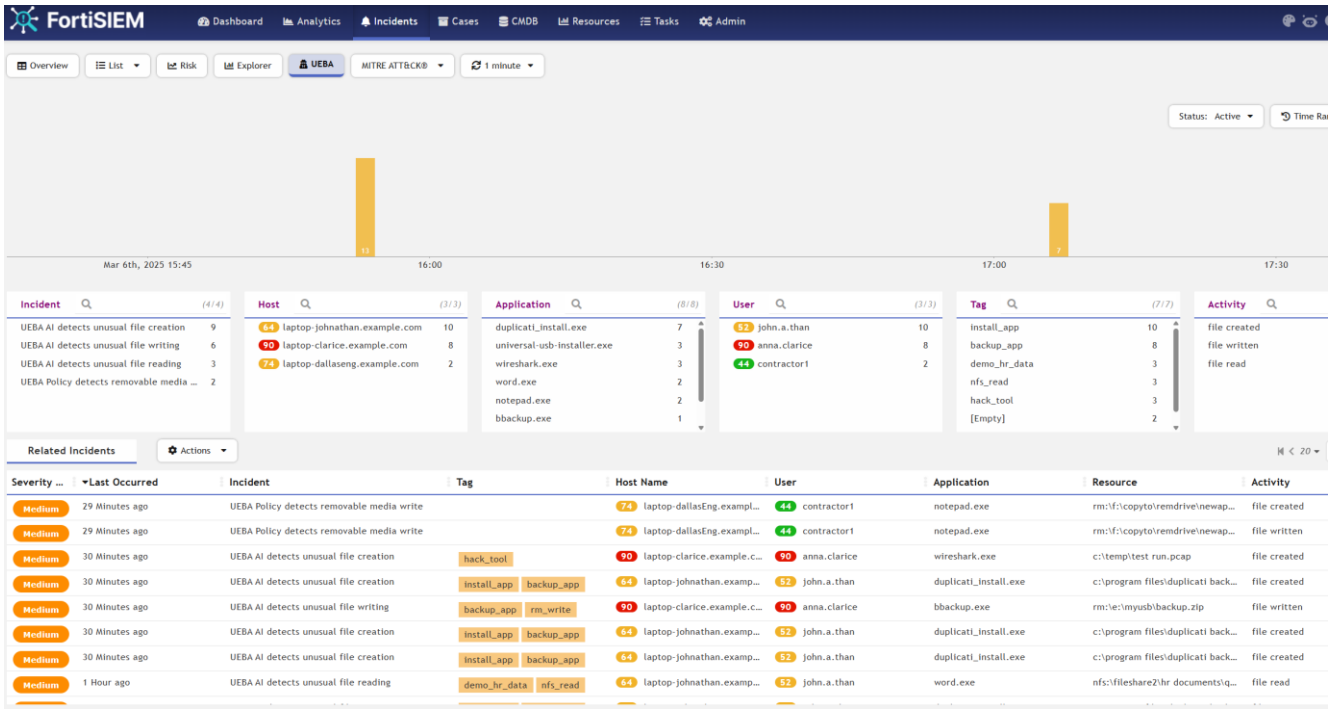

Рис. 3.6. Вкладка *UEBA*

Перегляд MITRE ATT&CK (рисунок 3.7) надає дані для інформаційних технологій (IT) і промислових систем управління (зведені відомості про ICS), вибравши IT або ICS перед наступними доступними типами переглядів:

перегляд покриття правил;

висвітлення інцидентів;

перегляд огляду інцидентів MITRE ATT&CK.

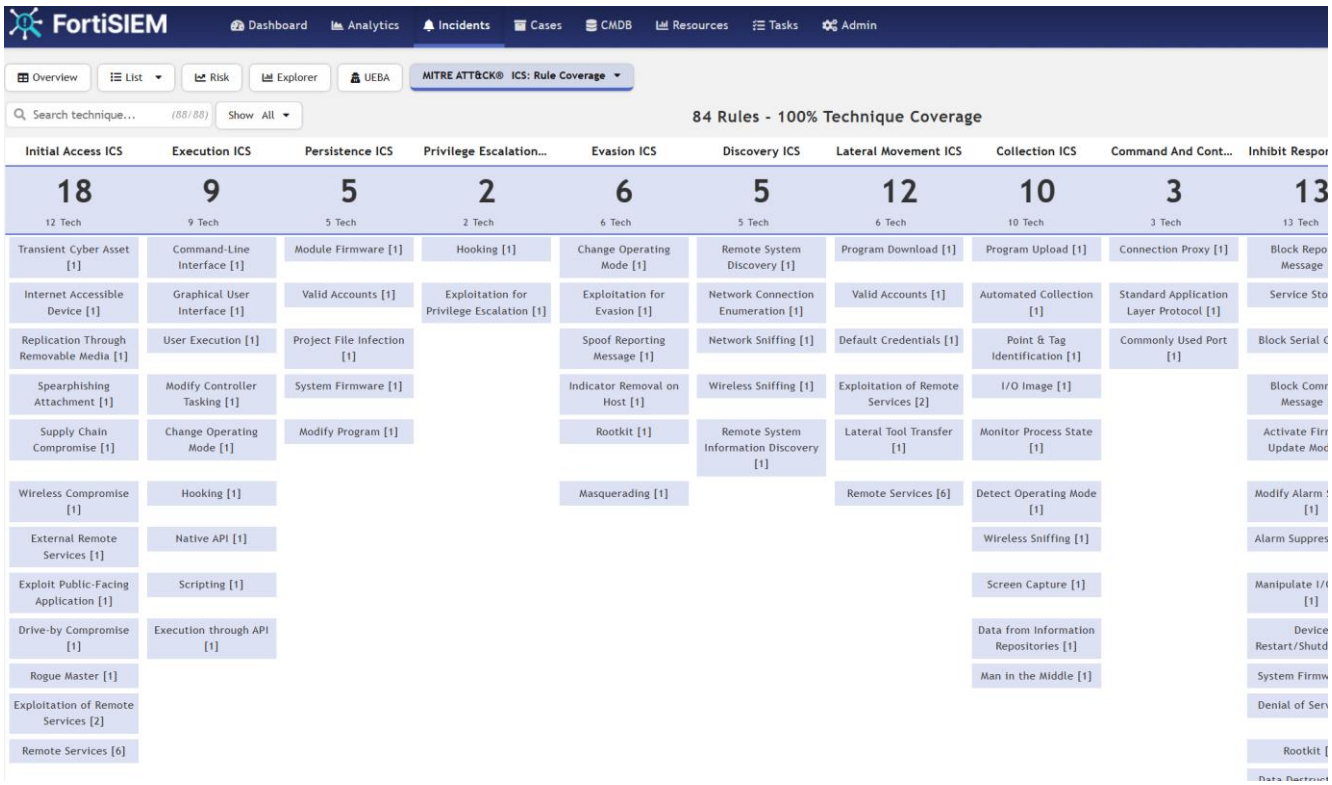

Рис. 3.7. Вкладка *MITRE ATT&CK*

Розглянемо порядок розслідування інцидентів.

Ми можемо детально вивчити інцидент за допомогою таких методів.

1. На сторінці *Incidents* вибрати інцидент і вибрати *Investigate* зі спадного списку *Action*.

або

2. На сторінці *Analytics* > *Investigation* введіть ідентифікаційний номер інциденту, який ми хочемо дослідити, або вибрати його з 10 найпопулярніших інцидентів (рисунок 3.8), які спочатку з’являться на новій вкладці, і натисніть *Load*.

Якщо вказано номер інциденту, на сторінці дослідження *Analytics* відображатиметься неорієнтований граф інциденту та залучених об’єктів (хост/IP, користувач, процес, файл) як вузли (рисунок 3.9). Останні 10 найпопулярніших інцидентів спочатку з’являються на новій вкладці на сторінці *Analytics* > *Investigation*.

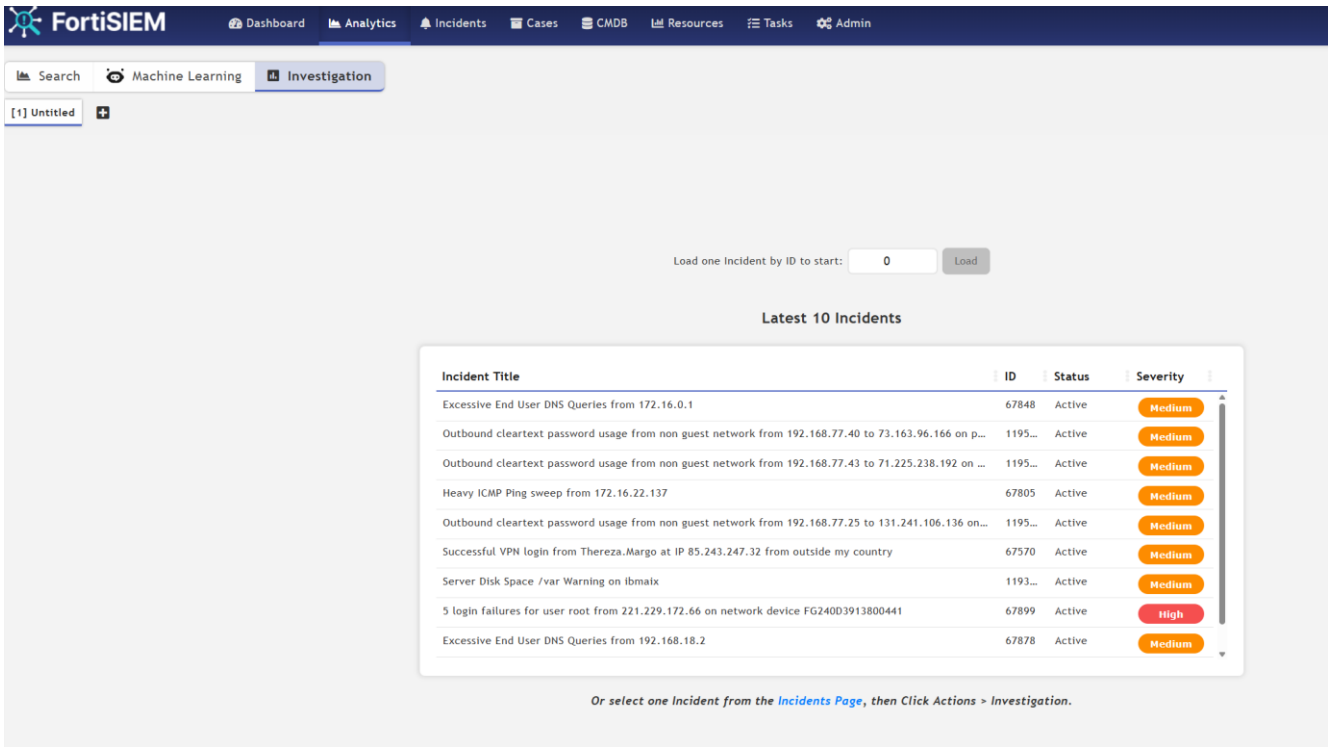

Рис. 3.8. Вкладка *Analytics* > *Investigation*

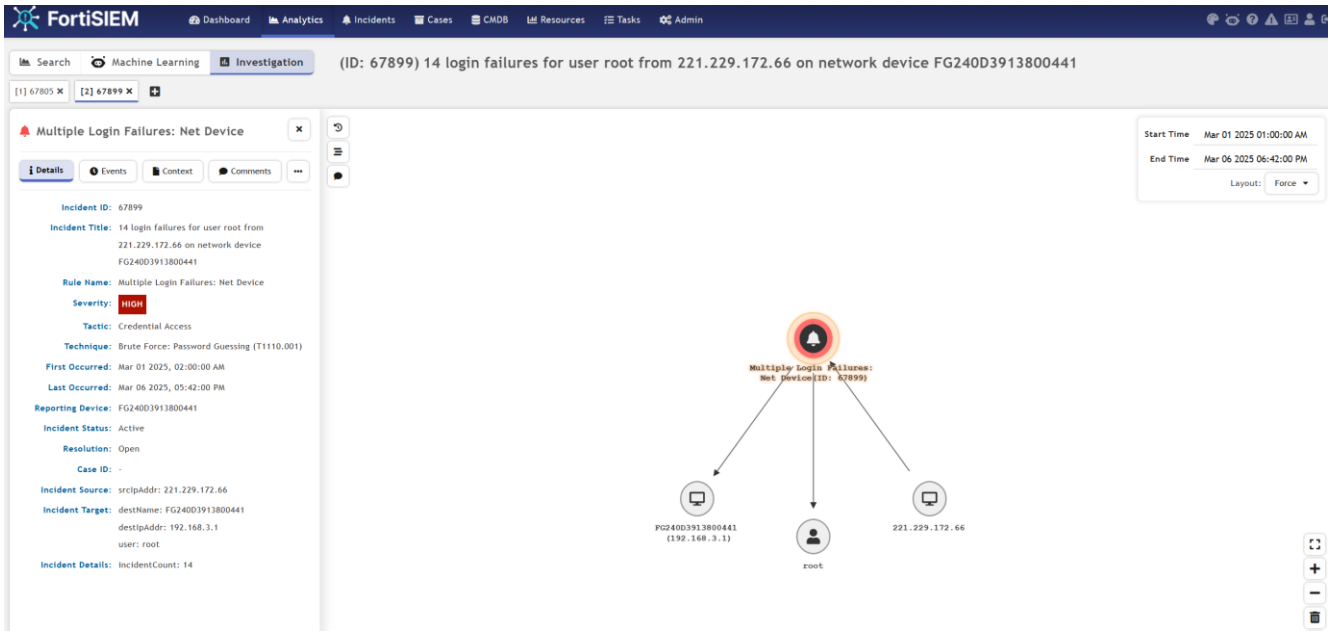

Рис. 3.9. Граф інциденту та залучених об’єктів

Ми проводимо дослідження інциденту та пов’язаних з ним об’єктів. Після завантаження інциденту в *Analytics* ми можемо виконати наведені нижче дії. Вузол буде або інцидентом, або сутністю (хост/IP, користувач, процес, файл). Інцидент можна розпізнати за кольоровою рамкою, яка також вказує на

серйозність інциденту.

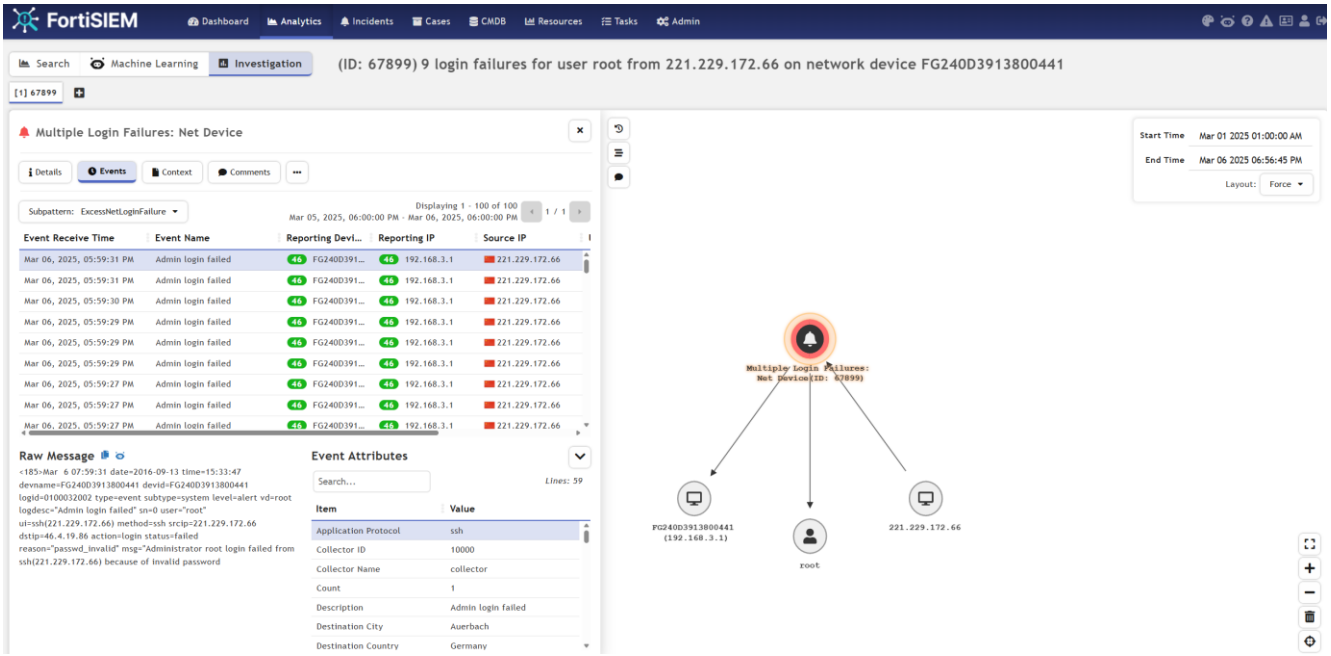

Рис. 3.10. Детальна інформація про інцидент безпеки

Необхідно навести курсор на вузол, щоб відкрити швидкий огляд об’єкта інциденту/сутності.

Необхідно клацнути на вузол інциденту, щоб отримати доступ до лівої панелі, яка містить детальну інформацію про інцидент і різні дії, які ми можемо виконати.

3.3. Рекомендації щодо виявлення загроз корпоративним інформаційним ресурсам і реагування на них

Ефективна стратегія виявлення та реагування на загрози корпоративним інформаційним ресурсам дозволить організаціям захистити себе від кібератак, постійно здійснюючи моніторинг своїх мереж та додатків на наявність підозрілої активності та вживаючи швидких заходів для зменшення будь-яких потенційних загроз. Однак розробка такої стратегії вимагає певних зусиль. Щоб випереджати зловмисників, організація повинна, серед іншого, впроваджувати складні технології, розробляти чіткі плани комунікації та інвестувати в постійне навчання

співробітників.

Мета виявлення загроз та реагування на них полягає у виявленні потенційних загроз та їх нейтралізації якомога раніше, в ідеалі до того, як буде завдано будь-якої шкоди. Процес починається зі збору даних з різних джерел, таких як мережевий трафік, системні журнали та пристрої безпеки.

Потім ці дані аналізуються для виявлення будь-яких аномалій або підозрілої поведінки, які можуть свідчити про потенційну кіберзагрозу. Це вимагає використання передових алгоритмів розвідки загроз та машинного навчання, які можуть визначати закономірності та аномалії у великих наборах даних, допомагаючи виявляти загрози, які можуть бути пропущені традиційними заходами безпеки. З точки зору персоналу, це також вимагає кваліфікованого персоналу, культури безпеки та чітко визначених процесів і процедур, які регулярно тестуються та оновлюються, щоб випереджати нові загрози.

Після виявлення загрози починається фаза реагування. Це включає вжиття відповідних заходів для стримування загрози та зменшення будь-якої шкоди, яка вже могла бути завдана. Це може включати ізоляцію уражених систем або пристроїв, блокування шкідливого трафіку та видалення будь-якого виявленого шкідливого коду або програмного забезпечення. Загалом, ефективний процес виявлення загроз та реагування на них може мінімізувати вплив кібератак та захистити конфіденційні дані та критично важливі системи від пошкоджень.

Організації можуть використовувати різноманітні методи для підвищення рівня виявлення загроз та посилення захисту від кіберзлочинності. *Основними рекомендаціями щодо виявлення загроз корпоративним інформаційним ресурсам можуть бути:*

Використовуйте розширену аналітику загроз. Розширена аналітика загроз передбачає використання автоматизованих інструментів для моніторингу та аналізу даних про загрози з різних джерел, включаючи мережеві журнали, канали подій безпеки та звіти про аналіз шкідливих програм. Застосовуючи до цих даних розширену аналітику та алгоритми машинного навчання, ці інструменти можуть виявляти закономірності та аномалії, щоб швидко позначити потенційну загрозу.

Це дозволяє організаціям швидко реагувати на будь-яку підозрілу активність.

Регулярно проводьте оцінку вразливостей. Кіберзахист настільки міцний, наскільки міцне його найслабше місце. Регулярно скануючи корпоративні системи, мережі та додатки на наявність відомих вразливостей, можна виявити слабкі місця у корпоративних системах, перш ніж ними скористаються зловмисники. Також можна запропонувати командам безпеки знайти прогалини у власному кіберзахисті за допомогою внутрішніх командних навчань, що завершуються остаточним тестом проти шкідливих дій. Звідти можна виявити та усунути прогалини у безпеці за допомогою таких дій, як встановлення виправлень, оптимізація стеку безпеки або впровадження додаткових засобів контролю безпеки.

Необхідно визначати та встановлювати базову поведінку. Легше виявити зловмисників, які проникли у корпоративні системи, якщо ви знаєте, як виглядає звичайна мережева та системна активність. Щоб розробити базовий профіль поведінки, ваші команди безпеки можуть дослідити такі точки даних, як потік трафіку, доступ до даних та використання додатків, а також позначити шаблони, які є поширеними та очікуваними. Це дозволяє організації швидко виявляти будь-яку незвичайну активність, яка може свідчити про потенційну загрозу.

Використовуйте штучний інтелект та машинне навчання. Штучний інтелект та машинне навчання можуть покращити стратегію виявлення загроз, дозволяючи організаціям автоматизувати аналіз величезних обсягів даних. Зокрема, однією з переваг штучного інтелекту та машинного навчання є їхня здатність виявляти раніше невідомі загрози. Традиційні інструменти безпеки часто обмежуються виявленням відомих загроз на основі попередньо визначених правил або сигнатур. Натомість штучний інтелект та машинне навчання можуть навчатися на історичних даних та виявляти нові загрози на основі їхніх моделей поведінки, навіть якщо вони ніколи раніше не спостерігалися. Крім того, штучний інтелект та машинне навчання можуть допомогти відфільтрувати сигнал від шуму у ваших сповіщеннях безпеки, зменшуючи кількість хибнопозитивних результатів та позначаючи найбільш релевантні сповіщення для подальшого розслідування

командою безпеки.

Коли йдеться про захист організації від кібератак, виявлення – це лише перший крок. Команди з кібербезпеки також повинні вживати швидких та рішучих заходів для ізоляції загроз, зменшення збитків та усунення будь-яких основних вразливостей, виявлених внаслідок атаки. Цього можна досягти найлегше, якщо дотримуватися трифакторного підходу до кібербезпеки, що включає людей, технології та процедури. Плануючи заздалегідь та інвестуючи в правильні інструменти та практики, ми можемо забезпечити свою організацію готовністю до швидкого та ефективного реагування на загрози.

Основними рекомендаціями щодо реагування на загрози корпоративним інформаційним ресурсам можуть бути:

Необхідно розробляти та тестувати План реагування на інциденти. План реагування на інциденти окреслює кроки, які організація вживатиме у разі кібератаки. Щоб розробити свій план, почніть з визначення обсягу та цілей, виявлення потенційних загроз та розподілу ролей і обов'язків між учасниками. Після того, як ці рекомендації будуть встановлені, протестуйте їх, проводячи регулярні навчання та тренування, щоб переконатися, що план ефективний та актуальний. Ви можете підвищити реалістичність цих навчань, розгорнувши їх у контрольованому середовищі, такому як кіберполігон, який імітує унікальний технологічний стек конкретної організації.

Необхідно встановити чіткі протоколи комунікації. Коли будь-яка організація зазнає кібератаки, час має вирішальне значення. Заздалегідь встановлено чіткі протоколи комунікації, що оптимізують реакцію га інцидент та забезпечують якомога швидше усунення загроз. Ваш протокол має передбачати шляхи ескалації та канали зв'язку для ключових зацікавлених сторін, включаючи зовнішні сторони, такі як клієнти, партнери та регуляторні органи. Плануючи заздалегідь, як спілкуватися під час сценарію термінової загрози, ви збільшите свої шанси виявити загрозу, перш ніж вона завдасть значної шкоди.

Необхідно ізолювати та стримувати загрози. Після виявлення загрози першим кроком має бути її ізоляція, щоб запобігти її поширенню та полегшити

усунення наслідків. Корпоративний План реагування на інциденти повинен включати кроки для швидкої ідентифікації уражених систем, відключення їх від Інтернету та карантину уражених доменів. Ви можете спростити процес стримування, вживши превентивних заходів, таких як сегментація мережі, щоб обмежити вплив атаки та забезпечити наявність та актуальність резервних копій, щоб ви могли швидко відновити системи у разі втрати даних.

Необхідно усувати причини інцидентів. Усунення наслідків передбачає вжиття заходів для усунення причини кібератаки та запобігання її повторенню. Після локалізації інциденту слід ретельно розслідувати атаку та визначити, як вона сталася. За допомогою виявленої інформації ви можете вжити відповідних коригувальних заходів, які можуть включати такі кроки, як виправлення вразливостей, оновлення політик безпеки або проведення додаткового навчання співробітників.

Необхідно навчати співробітників процедурам реагування. Навчання співробітників процедурам реагування на загрози є надзвичайно важливим для того, щоб вони розуміли свої обов’язки у разі кібератаки. Це може допомогти забезпечити скоординовану та ефективну відповідь, зменшуючи ризик подальшої шкоди для організації. Окрім надання чітких інструкцій щодо реагування на потенційні загрози, слід регулярно проводити навчальні сесії, включаючи вправи з кіберполігону, які дозволяють співробітникам практикуватися в реалістичних сценаріях. Також важливо забезпечувати постійні освітні та інформаційні програми, щоб корпоративна команда з кібербезпеки була в курсі останніх загроз.

Необхідно розуміти, що кіберзагрози продовжують збільшуватися та розвиватися. Питання не в тому, чи постраждає організація, а в тому, коли це відбудеться. Постійне приділення уваги питанням надійного виявлення та реагування на загрози забезпечить швидке припинення атак, мінімізуючи збитки, захищаючи корпоративні дані та забезпечуючи безперервність бізнесу.

Встигати за постійно мінливим ландшафтом загроз та новітніми технологіями може бути складним завданням, що вимагає постійного вдосконалення кібербезпеки.

ВИСНОВКИ

В роботі досліджено проблему виявлення загроз корпоративним інформаційним ресурсам і реагування на них. Встановлено, що для захисту корпоративних інформаційних ресурсів необхідно безперервно відстежувати та аналізувати стан мережі та кінцевих пристроїв, щоб швидко виявляти та реагувати на потенційні кіберзагрози. Цей підхід, що поєднує методи та засоби, процедури та аналітику, забезпечує захист від відомих і нових ризиків. SIEM системи відіграють важливу роль у виявленні та реагуванні на загрози корпоративним інформаційним ресурсам.

Визначено існуючі підходи до виявлення загроз корпоративним інформаційним ресурсам і реагування на них. Організації використовують різноманітні інструменти та процеси для ефективного виявлення загроз та реагування на них. SIEM – це тип програмного забезпечення, яке збирає, контролює та аналізує дані, пов’язані з безпекою, з різних джерел, таких як мережеві пристрої, сервери, додатки та системи. Воно забезпечує видимість та аналітику подій, загроз та інцидентів, пов’язаних з безпекою, у режимі реального часу, дозволяючи організаціям виявляти, реагувати та запобігати порушенням безпеки.

Проаналізовано існуючі рішення для виявлення загроз корпоративним інформаційним ресурсам і реагування на них. SIEM використовують попередньо визначені правила для генерації сповіщень та надають можливості реагування на інциденти. Найкраще програмне забезпечення SIEM сьогодні еволюціонувало та включає аналітику поведінки користувачів та об’єктів. Вони стають основним елементом для сучасних команд SOC для різних сценаріїв моніторингу безпеки та управління відповідністю вимогам.

Проаналізовано методи та засоби виявлення загроз корпоративним інформаційним ресурсам і реагування на них на основі правил FortiSIEM. FortiSIEM – це вдосконалене рішення SIEM, яке поєднує розширений аналіз

журналів і трафіку з моніторингом продуктивності/доступності, аналізом змін і точним знанням інфраструктури для забезпечення точного виявлення загроз, усунення проблем, реагування на інциденти та звітування про відповідність. Кореляція розподілених подій і виявлення загроз системою FortiSIEM здійснюється механізмом правил.

В роботі розглянуто порядок створення правил рішення FortiSIEM для виявлення загроз корпоративним інформаційним ресурсам. Правила визначають умови, на які слід звернути увагу, і які викликають інцидент, коли ці умови виникають. FortiSIEM включає понад 500 визначених системою правил, а також є можливість створювати власні правила. В роботі розглянуто порядок роботи з інцидентами в середовищі рішення FortiSIEM.

Розроблено рекомендації фахівцям з кібербезпеки щодо виявлення загроз корпоративним інформаційним ресурсам і реагування на них.

Таким чином, ефективна стратегія виявлення та реагування на загрози корпоративним інформаційним ресурсам дозволить організаціям захистити себе від кібератак, постійно здійснюючи моніторинг своїх мереж та додатків на наявність підозрілої активності та вживаючи швидких заходів для зменшення будь-яких потенційних загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. IBM X-Force 2025 Threat Intelligence Index. URL: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index

2. What Is Threat Detection and Response (TDR)? Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-threat-detection-response-tdr

3. MITRE. 11 Strategies of a World-Class Cybersecurity Operations Center. /Kathryn Knerler, Ingrid Parker, Carson Zimmerman – The MITRE Corporation, 2022. – 452 p. URL: https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

4. Thuy Nguyen. Effective Threat Detection: What Is Threat Detection and Response (TDR)? Crowdstrike, February 20, 2025. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/threat-detection/

5. Phil Sweeney. What is threat detection and response (TDR)? Complete guide. TechTarget. URL: https://www.techtarget.com/searchsecurity/definition/threat-detection-and-response-TDR

6. A Solution Guide to Operational Technology Cybersecurity. White Paper. Fortinet. URL: https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/02_Collateral/WhitePaper/wp-A-Solution-Guide-to-Operational-Technology-Cybersecurity.pdf

7. FortiSIEM. Data Sheet. Fortinet. URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSIEM.pdf

8. FortiSIEM. User Guide 7.3.1. URL: https://help.fortinet.com/fsiem/7-3-1/Online-Help/HTML5/Home.htm

9. FortiSIEM. FortiSIEM Reference Architecture Using ClickHouse. 7.3.1. URL: https://docs.fortinet.com/document/fortisiem/7.3.1/fortisiem-reference-architecture-

using-clickhouse/105365/what-is-the-fortisiem-reference-architecture

10. Top 10 SIEM Tools For 2025. By SentinelOne. Updated: May 2, 2025. URL: https://www.sentinelone.com/cybersecurity-101/data-and-ai/siem-tools/

11. Best SIEM Solutions: Top 10 SIEM systems and How to Choose. Exabeam. URL: https://www.exabeam.com/explainers/siem-tools/siem-solutions/

12. 2024 Gartner Magic Quadrant for SIEM. URL: https://www.splunk.com/en_us/form/gartner-siem-magic-quadrant.html

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)