ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення та реагування на кіберінциденти в інформаційній системі організації на базі AlienVault OSSIM»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач(ка) вищої освіти групи БСДМ-63
КИЯШКО Євгеній
(ПРІЗВИЩЕ, Ім'я)

Керівник: ГАХОВ Сергій
к.Військ.н., доцент (ПРІЗВИЩЕ, Ім'я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

OSSIM - Open Source Security Information and Event Management

SIEM - Security Information and Event Management

VPC - Virtual Private Cloud

OTX - Open Threat Exchange

SSH - Secure Shell

SMTP - Simple Mail Transfer Protocol

MTA - Mail Transfer Agent

STARTTLS - Secure protocol for data exchange between mail servers through encrypted TLS connection.

SASL - Simple Authentication and Security Layer

IP - Internet Protocol

NVT - Network Vulnerability Testing

DLP - Data Loss Prevention

IPS - Intrusion Prevention System

IDS - Intrusion Detection System

ВСТУП

Актуальність дослідження. Інформація сьогодні є важливим активом для будь-якого підприємства, зокрема через можливості, які забезпечують сучасні інтернет-технології для її використання у розвитку та збільшенні прибутковості бізнесу. Однак ці технології також відкривають простір для зловмисників, підвищуючи рівень уразливості інформаційних систем і мереж.

Сучасні кіберзагрози набагато складніші і серйозніші, ніж багато людей можуть собі уявити. За останні п'ять років світові компанії стали свідками масштабних кібератак, таких як BlackEnergy, TeleBots, CryptoLocker, GreyEnergy, Industroyer, Petya і NotPetya, BadRabbit, Buhtrap, WannaCry, TeslaCrypt, Nyetya. Ці атаки спрямовані на підприємства критичної інфраструктури, енергетичний сектор, фінансові організації, транспортні та логістичні компанії, медичні та фармацевтичні фірми, а також софтверні компанії.

З урахуванням цього можна зробити висновок, що жодне підприємство не може повністю застрахувати себе від потенційних матеріальних або фінансових втрат. Для забезпечення захисту підприємств від таких атак необхідно об'єктивно оцінити рівень захисту їхніх інформаційних систем. Аудит інформаційної безпеки є основним інструментом для контролю захисту інформаційних активів. Його результати, за умови професійного виконання, надають можливість створення комплексної та ефективної системи захисту, яка здатна впоратися із сучасними завданнями.

Впровадження комплексної системи захисту інформації (КСЗІ) на основі результатів аудиту інформаційної безпеки дозволяє здійснювати постійний контроль за системою, виявляти події, модифікації даних та невідкладно реагувати на них. Важливою частиною цього процесу є оптимізація аналізу журналів та записів, для чого використовуються системи управління інформацією про події та безпеки (SIEM). SIEM забезпечує аналіз подій в реальному часі, необхідний для виявлення та

реагування на небезпечні або незвичні події в області безпеки інформації. Тому тема кваліфікаційної роботи є актуальною.

Об'єкт дослідження – виявлення та реагування на кіберінциденти в інформаційній системі організації на базі AlienVault OSSIM.

Предмет дослідження – технологія виявлення та реагування на кіберінциденти в інформаційній системі на основі рішення AlienVault OSSIM.

Мета роботи – розробити варіант застосування технології виявлення та реагування на кіберінциденти в інформаційній системі на базі AlienVault OSSIM.

Наукові завдання:

- дослідити сутність проблеми виявлення та реагування на кіберінциденти в інформаційній системі організації;
- проаналізувати підходи до виявлення та реагування на кіберінциденти в інформаційній системі організації;
- проаналізувати існуючі методи та засоби виявлення та реагування на кіберінциденти в інформаційній системі організації;
- проаналізувати методи та засоби виявлення та реагування на кіберінциденти в інформаційній системі організації на базі AlienVault OSSIM.

Методи дослідження – опрацювання літератури з даної теми, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано варіант застосування технології виявлення та реагування на кіберінциденти в інформаційній системі організації на базі AlienVault OSSIM, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2023 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ КОНТРОЛЮ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ

1.1. Аналіз потенційних небезпек та ризиків комп'ютерних мереж в інформаціній системі підприємства

Концепція ризику вважається ключовою у сфері безпеки загалом і, зокрема, інформаційної безпеки. Ризик інформаційної безпеки об'єднує широкий спектр питань, пов'язаних із загрозами для інформації, включаючи виявлення джерел загроз та вразливостей інформаційних технологій, а також визначення можливих наслідків реалізації загроз. Ризик також інтегрується у процеси техніко-економічного аналізу та ухвалення рішень, пов'язаних із забезпеченням інформаційної безпеки та створенням систем захисту інформаційних технологій.

Водночас зі змінами та ускладненням методів та засобів автоматизації процесів для роботи з інформацією збільшується залежність підприємництва від ступеню безпеки використовуваних ними інформаційних технологій .

Можна виділити чималий перелік джерел, що становлять загрози інформаційній безпеці підприємства:

- незаконна діяльність економічних структур у сфері використання інформації, її поширення та формування;
- порушення встановлених правил обробки, збору та передачі інформації;
- навмисні та ненавмисні дії користувачів інформаційних систем;
- помилки на етапі проектуванні інформаційних систем;
- невідповідність технічних засобів або збої програмного забезпечення в інформаційних системах.

На сьогоднішній день фахівцями з кібербезпеки досліджується досить широкий асортимент загроз безпеці інформаційних систем, які можна класифікувати за рядом ознак.

Рис. 1.1. Класифікація загроз безпеці інформаційної системи

Кожна з цих загроз може стати фатальною для підприємства. Витік важливої інформації, особистих даних співробітників чи клієнтів – все це може призвести до великих втрат, а , можливо, і до втрати бізнесу [2].

1.2 Методи та засоби технології виявлення та реагування на кіберінциденти в інформаційній системі організації

Під аспектом безпеки, термін "загроза" визначається як сукупність умов і факторів, які можуть потенційно призвести до порушення функціонування комп'ютерної мережі в цілому, включаючи контрольовані активи, такі як дані. Такі загрози можна класифікувати як умисні (ситуації, де шкода заподіюється свідомо) і природні. Перші охоплюють несанкціоновані підключення, виток інформації, порушення функціонування мережі, в той час як до других відносяться форс-мажорні обставини, нещасні випадки та помилки, що виникають внаслідок збоїв апаратури. Значна кількість вразливостей безпеки пов'язана з людським фактором, таким як недостатня компетенція користувачів або ігнорування інструкцій, наприклад, щодо парольної політики.

Аналіз комп'ютерної мережі вимагає уваги до всіх типів загроз і вразливостей. Загрози природного характеру зазвичай легше визначити з точки зору ризиків і захист від них не потребує глибокого аналізу. Проте, загрози, що походять від людського фактору, вимагають особливої уваги, оскільки неможливо передбачити дії людини навіть у випадках, коли відсутні мотиви та наміри втілити загрозу. З іншого боку, людський фактор набуває важливості у випадках, коли дисфункція системи може загрожувати безпеці людини, що набуває особливого значення з футуристичного погляду, оскільки майбутнє, коли робототехніка стане повсякденною, вважається недалеким часом.

NIST Cybersecurity Framework4 (Платформа кібербезпеки Національного інституту стандартів та технологій (NIST)) може допомогти організації розпочати або вдосконалити свою програму кібербезпеки. Ця Платформа створена на основі відомих ефективних практик та може допомогти організаціям підвищити рівень кібербезпеки. Вона сприяє комунікації між внутрішніми та зовнішніми зацікавленими сторонами щодо питань забезпечення кібербезпеки, і допомогає більшим організаціям краще

інтегрувати та узгоджувати управління ризиками кібербезпеки з більш широкими процесами управління ризиками підприємства так, як це описано в серії NISTIR 82865.

Платформа організована за п'ятьма ключовими функціями – ідентифікація, захист, виявлення, реагування та відновлення. Ці п’ять добре відомих термінів, якщо їх розглядати разом, надають комплексне уявлення щодо життєвого циклу управління ризиками кібербезпеки.

Рис. 1.2. Стандарт NIST [5]

Розпізнавання

Документо-інформаційні потоки – важливо не лише розуміти, який тип інформації збирає та використовує Ваше підприємство, але також розуміти, де знаходяться ці дані та як вони використовуються, особливо якщо це стосується контрактів та зовнішніх партнерів.

Інвентаризація апаратного та програмного забезпечень – важливо знати всі слабкості ваших комп’ютерів та ПЗ, оскільки саме вони найчастіше стають точками

входу для зловмисників. Інвентаризація може бути у такій простій формі, як електронні таблиці.

Встановлення правил кібербезпеки, що включатимуть ролі та обов'язки персоналу – ці правила та процедури мають чітко описувати Ваші очікування щодо того, як дії з кібербезпеки захищатимуть вашу інформацію та системи, а також як вони підтримуватимуть критичні процеси підприємства. Правила кібербезпеки мають бути інтегровані з іншими факторами ризику підприємства (наприклад, фінансовими, репутаційними тощо).

Виявляння загроз, факторів вразливості та ризиків стосовно активів – забезпечте розробку та керування процесами управління ризиками з метою гарантії того, що всі можливі внутрішні та зовнішні загрози виявлені, оцінені та внесені до реєстру загроз. Переконайтеся, що засоби реагування на ризики встановлені, пріоритезовані та відпрацьовані, а результати контролюються.

Для функції "Розпізнавання" компанії потребують інструменти, які можуть допомогти в розпізнаванні активів та оцінці ризиків.

Nmap: Це потужний інструмент мапінгу мережі, який може розпізнавати пристрої в мережі та виявляти відкриті порти та служби, які можуть бути вразливі до атак.

Програмне забезпечення для управління ризиками: інструменти, такі як RSA Archer та LogicGate Risk Cloud, можуть допомагати в ідентифікації та оцінці кібербезпекових ризиків.

Захист

Управління доступом до активів та інформації – забезпечте можливість створення унікальних облікових записів для кожного співробітника та гарантію того, що користувачі матимуть доступ лише до інформації, комп'ютерів і програм, які необхідні для їх роботи. Автентифікуйте користувачів (наприклад, за допомогою паролів та багатофакторних методів), перш ніж їм буде надано доступ до інформації,

комп’ютерів і програм. Ретельно контролюйте та відстежуйте фізичний доступ до пристроїв.

Захист конфіденційних даних – якщо ваше підприємство зберігає або передає конфіденційні дані, переконайтеся, що ці дані захищені шифруванням як під час їх зберігання на комп’ютерах, так і під час передачі іншим користувачам. Перевіряйте цілісность даних, щоб переконатися, що до них були внесені тільки схвалені зміни. Безпечно видаляйте та/або знищуйте дані, коли вони більше не потрібні або коли це не вимагається відповідними законами.

Регулярне створення резервних копій – багато операційних систем мають вбудовані можливості резервного копіювання; також існує програмне забезпечення та хмарні технології, які можуть автоматизувати процес резервного копіювання. Рекомендується зберігати один набір даних, який часто копіється, в автономному режимі для захисту від програм-вимагачів.

Захист своїх пристроїв – подумайте про встановлення брандмауерів на основному хості та інших засобах захисту, наприклад, кінцевих продуктах безпеки. Застосовуйте уніфіковані конфігурації пристроїв і контролюйте зміни в конфігураціях пристроїв. Деактивуйте служби або функції пристроїв, які не потрібні для підтримки ключових функцій. Переконайтеся, що існують правила щодо безпечного видалення пристроїв.

Управління факторами вразливості пристроїв – регулярно оновлюйте операційну систему та програми, встановлені на ваших комп’ютерах та інших пристроях, щоб захистити їх від атак. Якщо є можливість, активуйте автоматичне оновлення. Розгляньте можливість використання програмних засобів для сканування пристроїв на наявність додаткових факторів вразливості; усувайте вразливості з високою загрозою та/або впливом

Навчання користувачів – регулярно проводьте підготовку та перепідготовку усіх користувачів для підвищення їх обізнаності з корпоративними правилами та

процедурами кібербезпеки, а також їх особливими ролями та обов’язками, як умови працевлаштування.

Для функції "Захист" існують інструменти, які можуть допомагати в створенні бар'єрів проти потенційних кіберзагроз.

Брандмауери та системи запобігання вторгненням (IPS): Інструменти, такі як Cisco ASA, мережеві брандмауери Palo Alto Networks та Fortinet FortiGate, надають надійний захист мережі.

Антивірусне та анти malware-програмне забезпечення: Рішення, такі як Norton, Bitdefender або ESET, можуть допомагати захищати системи від шкідливого програмного забезпечення.

Інструменти контролю доступу: Інструменти, такі як Microsoft Active Directory або Okta, можуть допомагати керувати ідентифікацією користувачів та виконувати контроль доступу.

Сканування на вміст шкідливого програмного забезпечення перед підписанням: eSigner від SSL.com дозволяє сканувати документи на вміст шкідливого програмного забезпечення до надання електронних підписів, тим самим запобігаючи поширенню шкідливого коду через цифрово підписані документи.

Тестування

Тестування та оновлення процесів виявлення – забезпечте розробку та тестування процесів і процедур виявлення несанкціонованих суб'єктів та дій у мережах та у фізичному середовищі, включаючи діяльність персоналу. Персонал повинен знати про свої ролі та обов'язки щодо виявлення та пов'язаної звітності як у вашій організації, так і перед зовнішнім управлінням та юридичними органами.

Знайте очікувані потоки даних для вашого підприємства – якщо ви знаєте, які дані ваше підприємство планує використовувати і яким чином, то ви, швидше за все, помітите, коли станеться несподіване, а несподіване не може бути позитивним явищем, коли йдеться про кібербезпеку. Неочікувані потоки даних можуть включати експорт інформації про клієнтів із внутрішньої бази даних і вихід із мережі. Якщо ви

уклали контракт з постачальником хмарних або зовнішніх послуг, обговоріть з ним, як вони відстежують потоки даних і повідомляють про несподівані явища.

Ведення та моніторинг журналів – журнали мають вирішальне значення для виявлення аномалій у комп'ютерах та програмах вашого підприємства. Ці журнали фіксують такі події, як зміни в системах або облікових записах, а також ініціювання каналів зв'язку. Розгляньте можливість використання програмних засобів, які можуть агрегувати ці журнали, і шукати закономірності або аномалії з очікуваної поведінки мережі.

Розуміння впливу подій кібербезпеки – якщо буде виявлено подію кібербезпеки, ваше підприємство має працювати швидко та ретельно, щоб зрозуміти широту та глибину впливу. Зверніться по допомогу. Надання інформації про подію відповідним зацікавленим сторонам допоможе вам зберегти вигідну позицію стосовно партнерів, органів нагляду та інших (потенційно включаючи інвесторів), а також покращити правила та процеси.

Інструменти виявлення допомагають виявляти потенційні кібербезпекові інциденти.

Intrusion-Detection-Systeme (IDS): Інструменти, такі як Snort або Suricata, можуть виявляти аномальну активність, яка може свідчити про атаку.

SIEM-інструменти (Security Information and Event Management): Платформи, такі як Splunk або LogRhythm, можуть агрегувати та аналізувати дані журналів з різних джерел для виявлення потенційних кібербезпекових інцидентів.

Реагування

Переконайтеся, що плани реагування перевірені – ще важливіше тестувати плани реагування, щоб переконатися, що кожна особа знає свої обов’язки щодо виконання плану. Чим краще підготовлена ваша організація, тим ефективнішим буде реагування. Це включає знання будь-яких правових вимог до звітності або необхідного надання інформації.

Переконайтеся, що плани реагування оновлені – тестування плану (та його виконання під час інциденту) неминуче виявить необхідні покращення. Забезпечте оновлення планів реагування з урахуванням отриманого досвіду.

Коли сталася подія, інструменти реагування допомагають організаціям швидко приймати заходи.

Платформи реагування на інциденти: інструменти, такі як IBM Resilient Incident Response Platform або D3 Security, можуть оптимізувати процес реагування на інциденти та забезпечити швидку та координовану реакцію.

Відновлення

Спілкування з внутрішніми та зовнішніми зацікавленими сторонами – відновлення багато в чому залежить від ефективної комунікації. У ваших планах відновлення потрібно враховувати, яка інформація як і коли буде передаватися різним зацікавленим сторонам, щоб усі вони отримували необхідну їм інформацію, а недоречна інформація не поширювалася.

Переконайтеся, що плани відновлення оновлені – як і у випадку з планами реагування, тестування виконання планів покращить обізнаність співробітників і партнерів, та виділить галузі, які потрібно вдосконалити. Обов’язково оновлюйте плани відновлення з урахуванням отриманого досвіду.

Інструменти відновлення допомагають компаніям відновити свої служби після кібербезпекового інциденту.

Резервне копіювання та відновлення даних: рішення, такі як Veeam або Veritas, можуть спростити процес відновлення даних після кібербезпекового інциденту.

Інструменти для аварійного відновлення: платформи, такі як Zerto або VMware Site Recovery, можуть допомагати компаніям відновити всю свою IT-інфраструктуру після серйозного інциденту [5].

1.3 Аналіз існуючих рішень SIEM-систем

Зважаючи на динамічність та постійно зростаючий обсяг кіберзагроз, вибір відповідного рішення для управління інформаційною безпекою стає стратегічно важливим завданням для будь-якої організації. Ринок систем управління інцидентами та подіями безпеки (SIEM) пропонує різноманітні продукти, а серед них особливо виділяються деякі лідери, зазначені у звітах Gartner.

Рис. 1.3. Магічний квадрант Gartner

1. Splunk Enterprise Security - це одна з провідних платформ в галузі, її особливістю є широкий перелік джерел інформації, з якими вона працює. Splunk Enterprise Security вміє збирати журнали подій з традиційних компонентів мережі

(серверів, засобів безпеки, шлюзів, баз даних і т. д.), мобільних пристроїв (смартфонів, ноутбуків, планшетів), веб-сервісів та розподілених джерел. Зібрана інформація включає дані про дії користувачів, журнали, результати діагностики тощо. Це дозволяє проводити зручний пошук та аналіз як в автоматичному, так і вручному режимі. Рішення має багато налаштовуваних сповіщень, які на основі зібраної інформації попереджають про наявні загрози та завчасно повідомляють про потенційні проблеми.

Продукт складається з декількох модулів, що відповідають за проведення розслідувань, логічних схем захищених ресурсів та інтеграцію з багатьма зовнішніми сервісами. Такий підхід надає можливість проводити детальний аналіз за багатьма параметрами та встановлювати взаємозв'язок між подіями, які на перший погляд не пов'язані одна з одною. Splunk Enterprise Security дозволяє порівнювати дані за часом, розташуванням, створюваними запитаннями, підключенням до різноманітних систем та іншими параметрами.

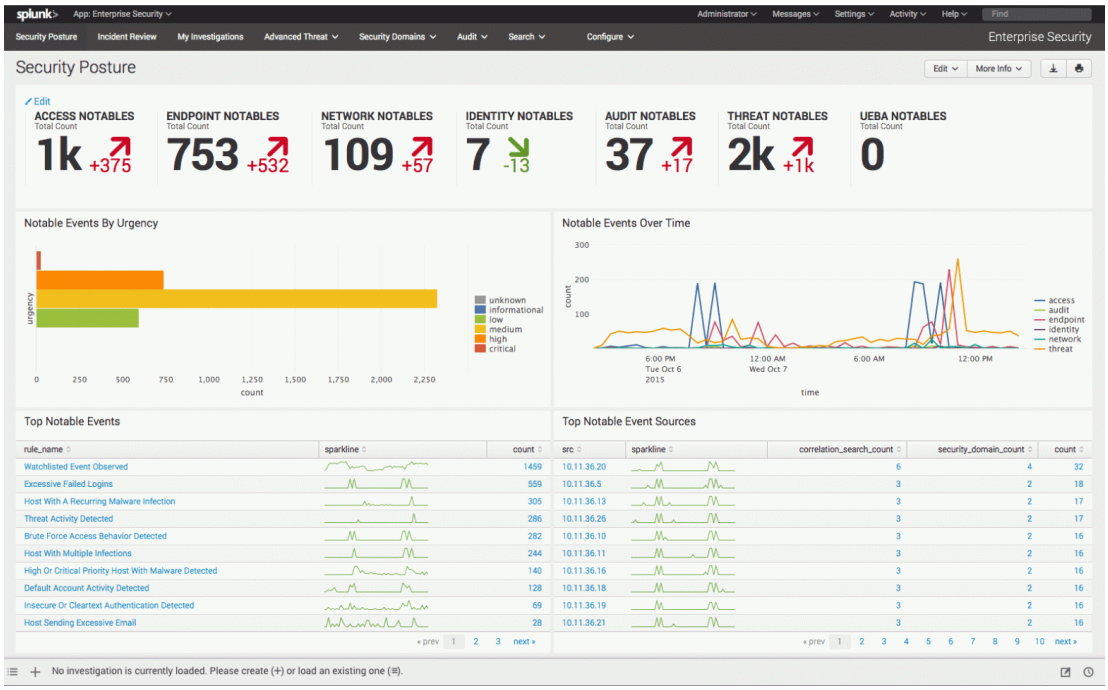


Рис. 1.4. Інтерфейс рішення Splunk

Інструмент також вміє працювати з великими об'ємами даних та є повноцінною платформою Big Data. Великі об'єми даних можуть оброблятися як у реальному часі, так і в режимі історичного пошуку, і підтримується велика кількість джерел даних. Splunk Enterprise Security може індексувати сотні терабайтів даних щодня, тому його можна використовувати в корпоративних мережах навіть дуже великих масштабів. Спеціальний інструмент MapReduce дозволяє швидко масштабувати систему горизонтально та рівномірно розподіляти навантаження, завдяки чому продуктивність системи завжди залишається на прийнятному рівні. При цьому користувачам доступні конфігурації для кластеризації та аварійного відновлення.

2. IBM QRadar Security Intelligence, є однією з найбільш передових на ринку: навіть у квадранті лідерів Gartner вона стоїть вище конкурентів, і вже 10 років поспіль потрапляє туди. Продукт складається з кількох інтегрованих між собою систем, які разом забезпечують максимальне охоплення подій в мережі, а багато функцій працюють прямо "з коробки". Інструмент може збирати дані з різних джерел, таких як операційні системи, пристрої безпеки, бази даних, додатки та багато інших.

QRadar Security Intelligence вміє сортувати події за пріоритетністю та виділяти ті, які несуть найбільшу загрозу безпеці. Це відбувається завдяки функціям аналізу аномальної поведінки об'єктів (користувачів, обладнання, служб та процесів в корпоративній мережі). Зокрема визначаються дії, пов'язані із зверненням до підозрілих IP-адрес або запитів з них. Щодо всіх підозрілих дій надаються детальні звіти, що, наприклад, дозволяє виявляти підозрілі дії в неробочий час. Такий підхід в поєднанні з функціями моніторингу користувачів та наочним представленням мережі на рівні додатків дозволяє боротися з загрозами внутрішніх агентів. Крім того, при звичайних кібератаках інформація надходить дуже швидко і дозволяє запобігти їм до того, як вони досягнуть мети і завдадуть значної шкоди.

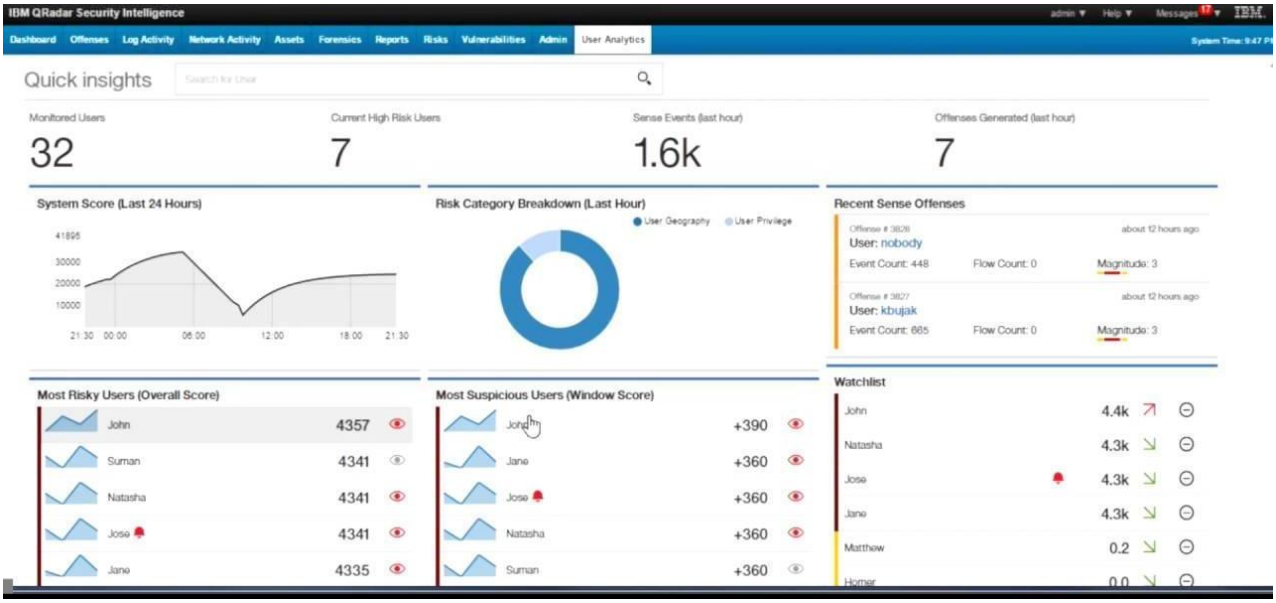


Рис. 1.5. Інтерфейс рішення IBM QRadar

Однією з головних особливостей IBM QRadar Security Intelligence є виявлення та встановлення пріоритетів на основі ризиків за допомогою розширеного аналізу та кореляції між активами, користувачами, мережевою активністю, наявними вразливостями, аналізом загроз і т. д. IBM Qradar може пов'язувати події в один ланцюжок, створюючи для кожного інциденту окремий процес.

Оскільки інформація збирається та виводиться на екран в одному місці, адміністратор може бачити всі пов'язані підозрілі дії, виявлені системою. Нові пов'язані події додаються в єдиний ланцюжок, так що аналітикам не потрібно перемикатися між кількома повідомленнями. А для більш глибоких розслідувань спеціальний інструмент IBM QRadar Incident Forensics може відновити всі мережеві пакети, пов'язані із зазначеним інцидентом, та поетапно відтворити дії зловмисника.

3. LogRhythm пропонує рішення SIEM наступного покоління для вирішення таких проблем, як фрагментовані робочі процеси, втома від сповіщень, сегментоване виявлення загроз, відсутність автоматизації, відсутність показників для визначення

зрілості та відсутність централізованої видимості. Воно пропонує різноманітні можливості для зберігання даних.

LogRhythm ідеально підходить для середнього бізнесу.

Ціна: високопродуктивний пристрій, програмне рішення та програма ліцензування Enterprise доступні за ціною. В інтернет-оглядах зазначено, що стартова ціна становить 28000 доларів.

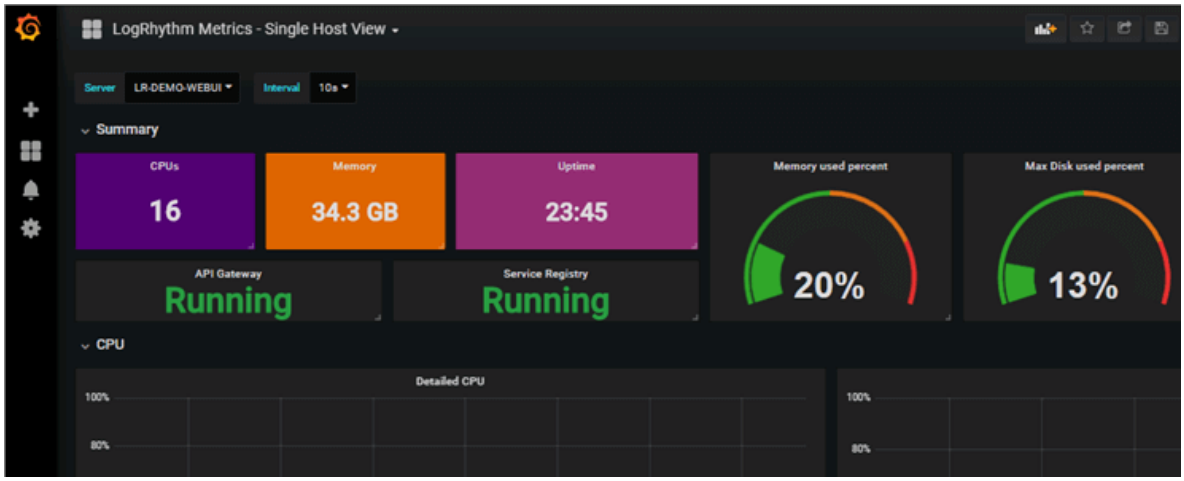


Рис. 1.6. Інтерфейс рішення LogRhythm

Нижче наведено деякі особливості LogRhythm:

- Єдине стандартизоване представлення, а також можливість обробки неструктурованих даних;
- Підтримуються Linux і Windows;
- Засновано на штучному інтелекті;
- Працює з широким спектром обладнання та форматів журналів.

Ця платформа містить всі функції та можливості, включаючи штучний інтелект, кореляцію журналів та поведінковий аналіз.

4. Securonix є хмарним рішенням SIEM (Система управління подіями та інформацією безпеки), яке використовує передові аналітичні та машинне навчання

для виявлення та реагування на загрози безпеки. Цей продукт пропонує широкі можливості для забезпечення безпеки та включає в себе такі ключові аспекти:

Аналітика поведінки користувачів та об'єктів: Securonix використовує аналіз поведінки користувачів та об'єктів для виявлення аномалій та надзвичайних подій. Це дозволяє вчасно розпізнавати потенційні загрози та атаки, враховуючи звичайний зразок користувальницького або об'єктного поведінки.

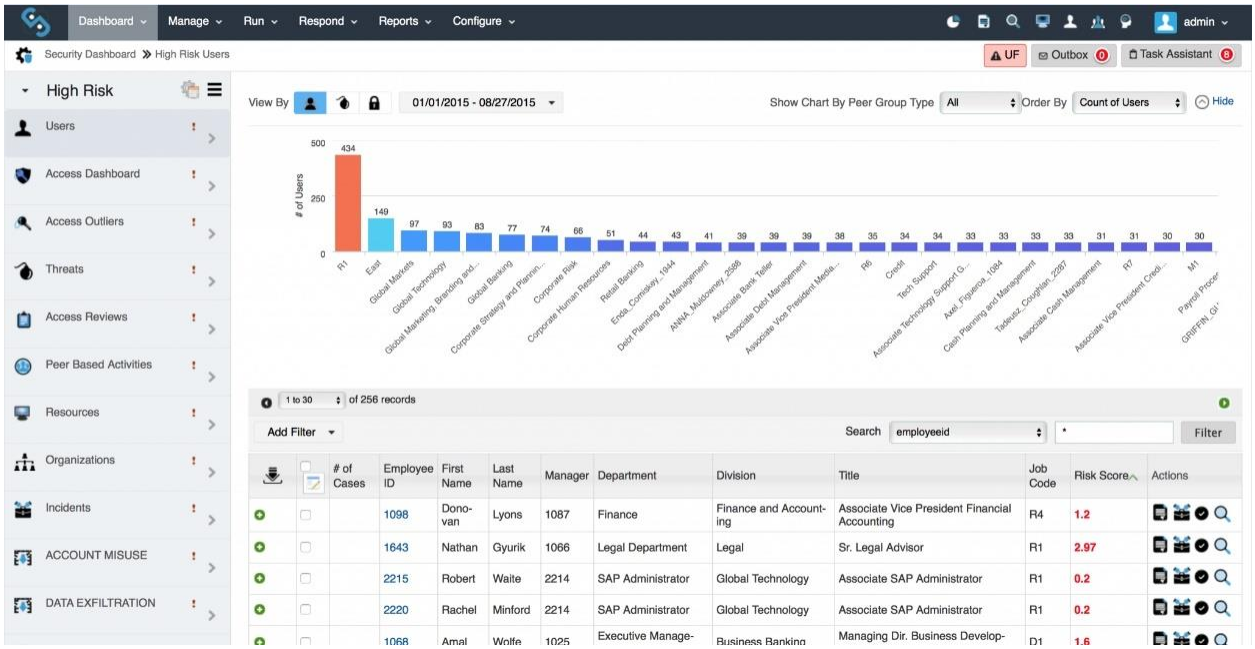


Рис. 1.7. Інтерфейс рішення Securonix

Автоматизація та оркестрація безпеки: Securonix вбудовує автоматизацію та оркестрацію в свої можливості. Це означає, що система може автоматично реагувати на виявлені загрози, вживаючи задані заходи безпеки. Це дозволяє швидше реагувати на інциденти та зменшує час реакції на потенційні небезпеки.

Машинне навчання: Securonix використовує технології машинного навчання для покращення ефективності виявлення загроз та аналізу подій. Система навчається

на основі реальних даних та стає все більш точною у виявленні нових та вдосконалення відповідей на загрози.

Хмарне рішення: Як хмарне рішення, Securonix надає гнучкість та масштабованість, що полегшує впровадження та управління системою безпеки. Це особливо важливо в умовах зростаючого обсягу даних та розподіленого характеру сучасних бізнес-середовищ.

Розширені функціональності: Securonix, ймовірно, має розширені можливості управління подіями та інформацією безпеки, зокрема в галузі візуалізації, аналізу та звітності, що допомагає адміністраторам та аналітикам забезпечувати ефективний контроль та реагування на події безпеки.

5. ArcSight ESM - це продукт SIEM для великих підприємств, які працюють у комерційних і регульованих секторах. Мікро Фокус підтримує модель розгортання програмного забезпечення на основі сервера, з якою ці організації відчувають себе комфортно. Основні можливості SIEM призначені для обробки та моніторингу великого спектру джерел даних в реальному часі. ArcSight ESM надає інформацію про загрози на основі подач від сторонніх постачальників. Оскільки він призначений для задоволення потреб підприємства, він може повідомляти дані за допомогою інтерфейсів або за допомогою широкого спектру звітів з відповідності до стандартів безпеки.

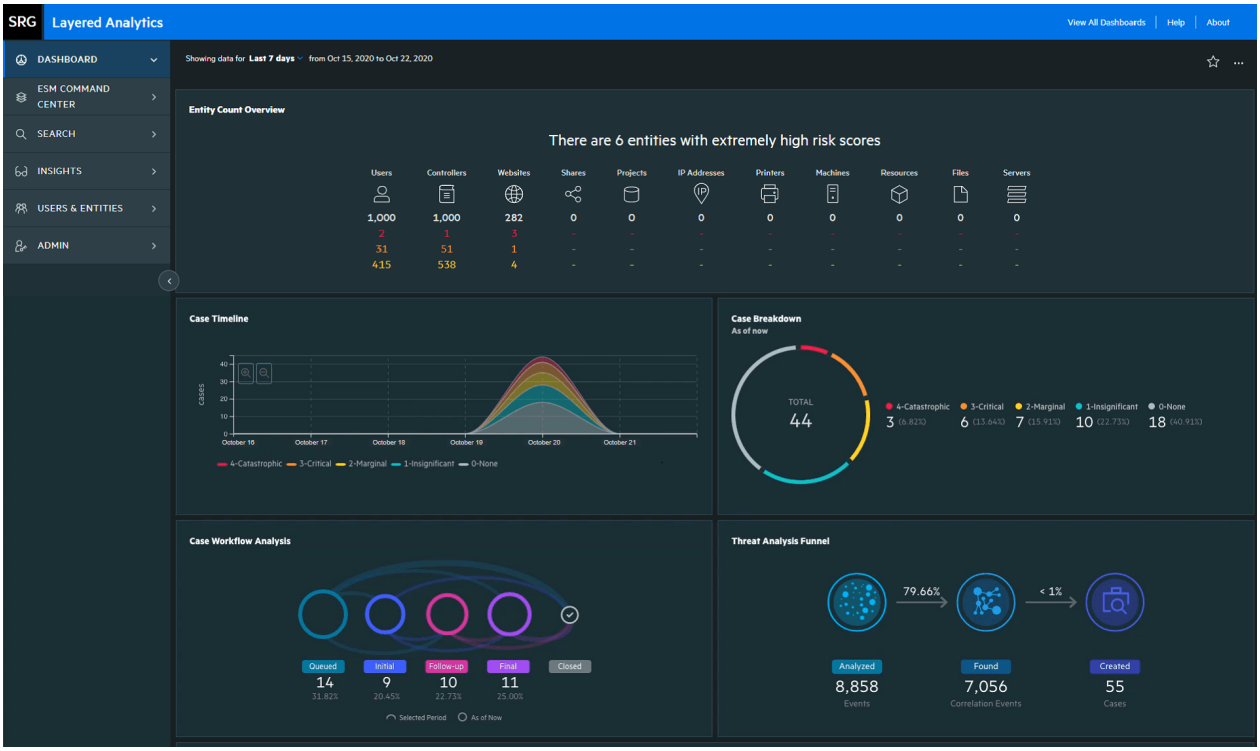


Рис. 1.8. Інтерфейс рішення ArcSight ESM

ArcSight ESM має багато переваг для великих організацій. По-перше, це зрілий продукт від компанії з довгою історією розробки та підтримки корпоративного програмного забезпечення. Як продукт, ArcSight ESM надає повноцінне рішення для корпорацій з великими національними та глобальними інфраструктурами. Крім того, він не тільки виявляє потенційні та фактичні загрози, але і включає необхідні інструменти для їх вирішення. Незважаючи на те, що ArcSight прагне надати повноцінне корпоративне рішення SIEM, в ньому є деякі недоліки. Він не надає мережевої форензіки, має обмежений логування хосту та заплутаний інтерфейс користувача. Крім того, це дорогий продукт, який вимагає значної підтримки та навчання. Основні характеристики та можливості цього продукту включають:

Виявлення та Реагування на Загрози в Реальному Часі: ArcSight надає засоби для виявлення потенційних загроз та подій в режимі реального часу. Це дозволяє організаціям оперативно реагувати на інциденти та миттєво вживати заходів безпеки.

Звітність про Відповідність: Один із ключових аспектів ArcSight - це здатність генерувати звіти про відповідність. Це важливо для відслідковування та дотримання стандартів безпеки та регуляторних вимог.

Управління Журналами: ArcSight дозволяє ефективно управляти журналами подій, що допомагає в аналізі та моніторингу подій безпеки. Це включає в себе зберігання, агрегацію та пошук подій для подальшого аналізу.

Аналітика Загроз: Рішення включає аналітичні засоби для виявлення загроз та аномальних подій. Штучний інтелект та машинне навчання можуть використовуватися для аналізу великих обсягів даних та виявлення складних загроз.

Інтеграція з Іншими Рішеннями: Micro Focus ArcSight може інтегруватися з іншими системами безпеки та інфраструктурними рішеннями для створення комплексної безпечної архітектури.

6. SolarWinds Security Event Manager - це рішення SIEM, спрямоване на виявлення та реагування на загрози в реальному часі. Його функціонал включає широкі можливості безпеки, такі як звітність про відповідність, управління журналами та аналітика загроз.

Це рішення дозволяє виявляти потенційні загрози в реальному часі, дозволяючи організаціям оперативно реагувати на інциденти безпеки. Забезпечує звітність про відповідність, що є важливим для відслідковування та дотримання стандартів безпеки та регуляторних вимог. Управління журналами дозволяє ефективно керувати подіями безпеки та забезпечує доступ до необхідної інформації для аналізу подій.

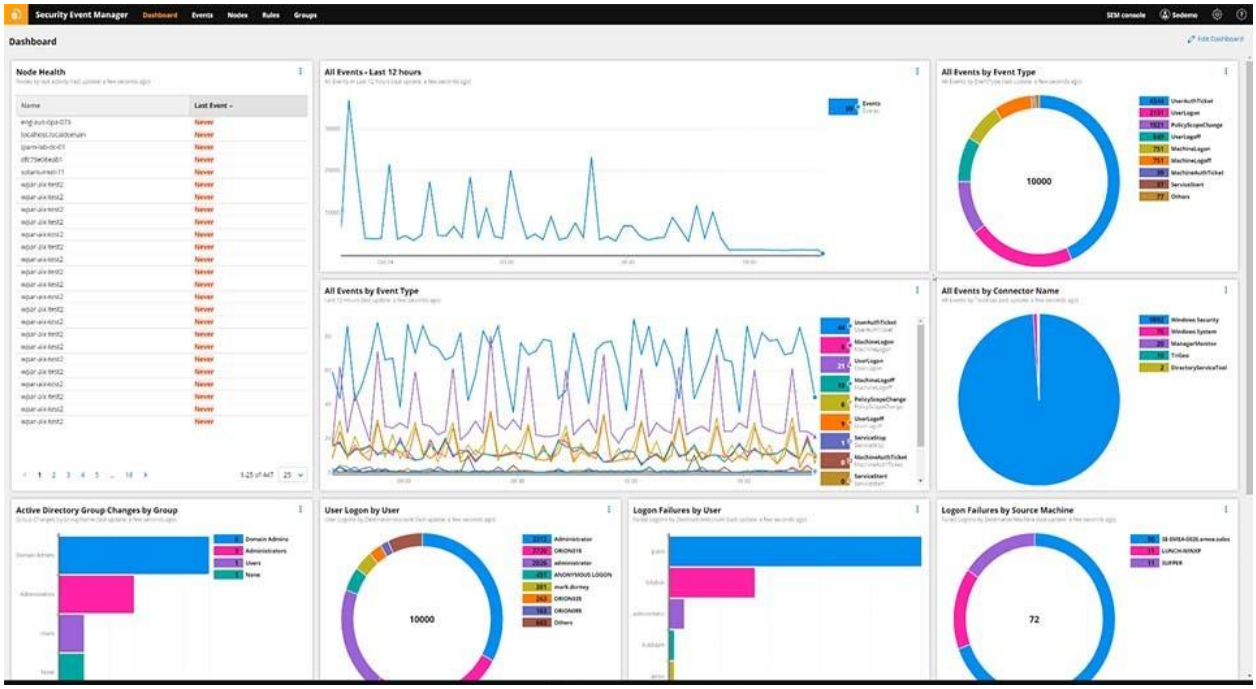


Рис. 1.9. Інтерфейс рішення SolarWinds Security Event Manager

Аналітика загроз є важливим компонентом SolarWinds Security Event Manager, допомагаючи виявляти аномалії та потенційні атаки. Це дозволяє швидше розпізнавати та відповідати на загрози безпеки.

Загалом, SolarWinds Security Event Manager пропонує комплексний набір інструментів для ефективного виявлення, відслідковування та реагування на загрози безпеки в реальному часі.

7. AlienVault Unified OSSIM, яка недавно об'єдналася з AT&T Business під брендом AT&T Security, проте її провідний продукт поки що продається під колишньою назвою. Цей інструмент, як і більшість інших платформ у відгуку, має більше функціональності, ніж традиційний SIEM. У AlienVault OSSIM є різноманітні модулі, відповідальні за контроль активів, повний захват пакетів та інше. Платформа також вміє проводити тестування мережі на наявність вразливостей, причому це може бути як одноразова перевірка, так і безперервний моніторинг. У випадку останнього,

повідомлення про наявність нової вразливості надходять майже одночасно з їх виникненням.

Рис. 1.10. Інтерфейс рішення AlienVault OSSIM

Серед інших можливостей платформи - проведення оцінки вразливостей інфраструктури, яке показує, наскільки мережа захищена, та чи відповідає її налаштування стандартам безпеки.

Платформа також вміє визначати атаки на мережу і своєчасно повідомляти про них. У цьому випадку адміністратори отримують докладну інформацію про те, звідки йде вторгнення, які частини мережі піддаються атакам і які методи використовують зловмисники, а також, що необхідно підприйняти для відбиття в першу чергу. Крім того, система вміє визначати інсайдерські атаки зсередини мережі та повідомляти про них.

За допомогою фірмового рішення AlienApps, платформа OSSIM може інтегруватися з рішеннями безпеки багатьох сторонніх виробників і ефективно доповнювати їх. Ці засоби також розширюють можливості AlienVault OSSIM у сфері налаштування безпеки та автоматизації реагування на загрози. Практично вся інформація про стан безпеки корпоративної мережі стає доступною безпосередньо через інтерфейс платформи. Ці інструменти також надають можливість автоматизувати та організовувати відповідні дії при виявленні загроз, що значно полегшує та прискорює їх виявлення та реагування на інциденти. Наприклад, при виявленні зв'язку з фішинговим сайтом адміністратор може відправити дані службі захисту DNS для автоматичного блокування цієї адреси, зробивши її недоступною для відвідування з комп'ютерів всередині організації.

2. АНАЛІЗ АРХІТЕКТУРИ ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ ALIENVAULT OSSIM

2.1 Призначення та функції SIEM системи в інформаційній системі організації

Поняття SIEM (Security Information and Event Management) в наші дні досить розмите, можна уявити, що це процес, який об'єднує мережну активність в єдиний адресний набір даних. Сам термін був придуманий Gartner у 2005 році, але з того часу саме поняття і все, що до нього відноситься, зазнало чимало змін. Спочатку абревіатура являла собою комбінацію двох термінів, що позначають область застосування програмного забезпечення: SIM (Security Information Management) – управління інформаційною безпекою та SEM (Security Event Management) – управління подіями безпеки .

SIM збирає всі дані в одному місці та забезпечує ефективне управління ними. SIM містить у собі функції централізованого журналювання, зберігання журналів, їх пошук і звітність, яка необхідна при проведенні аудиту. Управління подіями безпеки SEM дозволяє виявляти загрози та здійснювати управління ними. Функціонування SEM схоже на аналіз в реальному часі та використання правил кореляції для виявлення інцидентів. SEM також містить у собі функції управління інцидентами, які дають можливість адміністрування сервера і забезпечують функції безпеки. Більш структуровано функціонал SIEM наведено в табл. 2.1 .

За твердженням Gartner, SIEM-система повинна збирати, аналізувати та представляти інформацію з мережних пристроїв і пристроїв безпеки. Також у цю систему повинні входити додатки для управління ідентифікацією та доступом, інструменти управління вразливостями та бази даних і додатків.

Таблиця 2.1

Функціональність системи збору та кореляції подій (SIEM)

Підсистема SIM	Підсистема SEM
Управління інформаційною безпекою SIM	Управління подіями безпеки SEM
Централізоване журналювання	Аналіз погроз в режимі реального часу
Зберігання лог-файлів	Ідентифікація інцидентів
Пошук за лог-файлами та складання звітності	Можливості базового адміністрування серверів
	Дії з забезпечення безпеки

Для наочності виділимо кілька функцій, які зазвичай надаються SIEM-системами:

- можливість посилання попереджень на основі визначених налаштувань;
- звіти та логування для спрощення аудиту;
- можливість перегляду даних на різних рівнях деталізації.

SIEM збирає логи різних додатків, обробляє і зберігає в централізоване сховище, з яким зручно працювати. Зазвичай, розмір сховища залежить від кількості подій, що мають бути опрацьовані системою. Принцип збору та аналізу інформації системою SIEM добре ілюструє рис. 2.1.

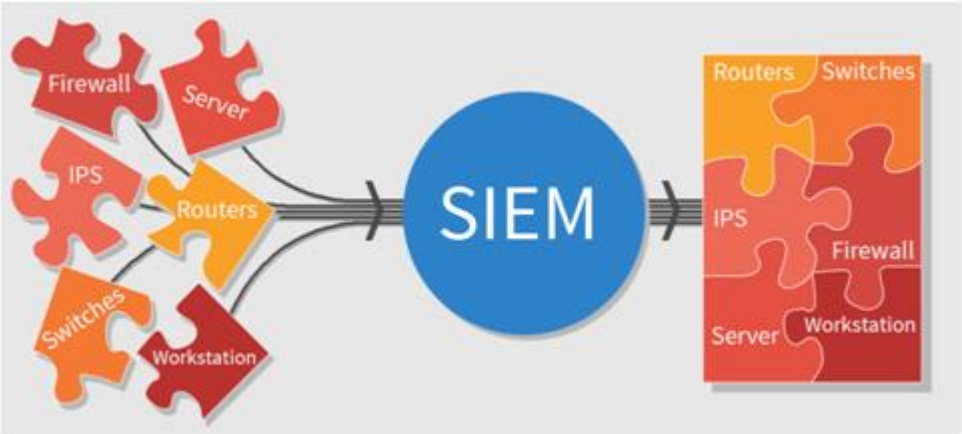


Рисунок 2.1. Принцип збору та аналізу інформації системою SIEM

SIEM-система може виявити можливу загрозу безпеки навіть якщо ця загроза добре замаскована під звичайну подію. Зробити це дозволяє те, що система аналізує не кожну окрему подію, а всі події в комплексі та таким чином може «побачити» повну картину подій зі сторони. Ця властивість може бути дуже корисною коли мова йде про систему аналізу загроз конфіденційній інформації користувачів відкритих соціальних мереж.

Така система призначена для аналізу інформації, що надходить від різних інших систем, таких як DLP, IDS, антивірусів і подальшого виявлення відхилення від норм за якимись критеріями. Як тільки виявлено відхилення – генерується інцидент. В основі роботи SIEM лежить, як не дивно, майже гола математика і статистика.

SIEM потрібна саме для збору та аналізу інформації. Інформація надходить з різних джерел – таких, як DLP-системи, IDS, маршрутизатори, міжмережеві екрани, АРМ користувачів, серверів.

Досить клопітно вручну переглядати логи з великої кількості джерел. До того ж бувають ситуації, коли зовні нешкідливі події, отримані з різних джерел, у сукупності несуть у собі загрозу. Припустимо, коли відбувається посилання листа з чутливими для компанії даними людиною, що має на це право, але на адресу, що знаходиться поза його звичайного кола адрес, на які він відправляє. DLP система цього може не

відловити, але SIEM, використовуючи накопичену статистику, на підставі цього вже згенерує інцидент. Аналогічно, якщо один з працівників IT відділу відкритої соціальної мережі почав провадити листування та повідомляти третім особам, що не мають допуску до інформації, відомості про користувачів, структуру соціальної мережі чи програмне та технічне забезпечення, що використовується для забезпечення роботи мережі, то це відразу буде помічено системою SIEM та адміністратори отримають відповідне сповіщення.

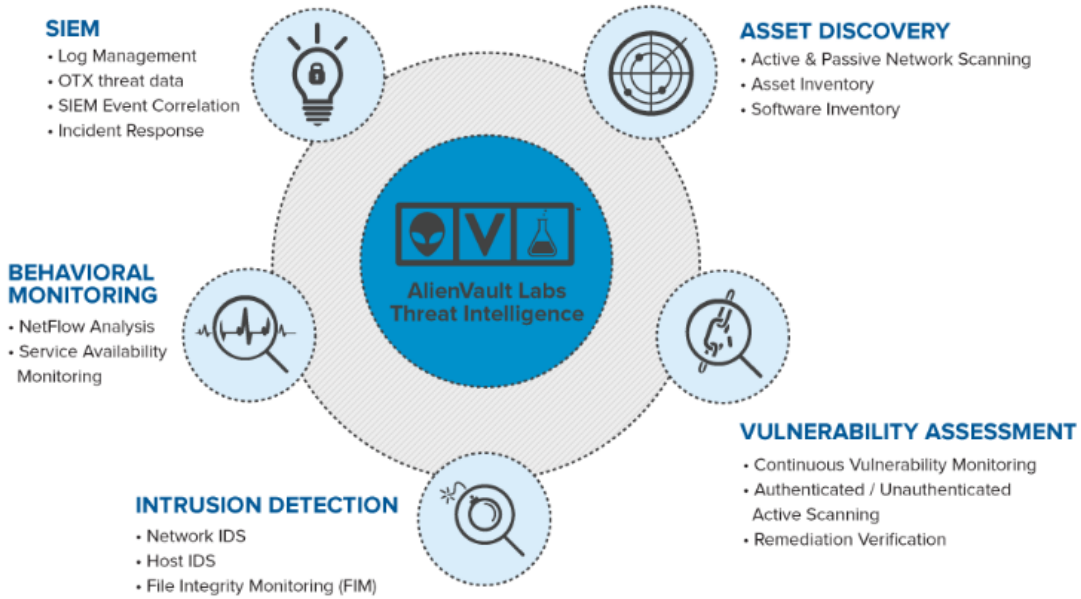


Рис 2.2 Можливості AlienVault OSSIM

Система SIEM може виконувати такі основні функції:

- аналізувати події та створювати оповіщення при якихось аномаліях: мережного трафіку, несподіваних дій користувача, невпізнаних пристроях і т. д.;
- перевірити на відповідність стандартам безпеки;
- створити красивий звіт. У тому числі налаштований безпосередньо для ваших потреб;

- відстежувати події, що спровоковані пристроями/серверами/критично важливими системами, створювати відповідні оповіщення для зацікавлених осіб;
- зібрати доказову базу з приводу інцидентів ;
- надати звіт про події в мережі без надання доступу до самої мережі, тобто адміністратор з відділу захисту інформації може відстежувати поведінку користувачів при тому, що не матиме ніякої можливості ознайомитися з конфіденційною інформацією власника аккаунту.

Загалом може скластися таке хибне враження, що SIEM-система є панацеєю для запобігання будь-яких загроз, але це не так. Ця система може відстежувати всі події в мережі, проте не може виконувати якихось дій крім створення попередження для адміністраторів цієї мережі, а адміністратор вже спираючись на отриманий звіт приймає рішення про подальші дії. Та все ж таки ця система може відстежувати поведінку користувачів та спираючись на статистику подій вирішити, чи потрібно адміністратору звернути більше уваги тому чи іншому користувачу. Причиною тому може бути як нетипова для користувача поведінка, так і певні маркери в повідомленнях, що можуть вказувати на можливу діяльність користувача, що пов’язана з тероризмом, розповсюдженням наркотичних речовин тощо.

До того ж система SIEM лише аналізує отримані дані і працює тим краще, чим більше до неї надходить інформації з різних джерел (IDS/IPS, DLP, маршрутизатори, сервери тощо) в вигляді логів.

Тобто на вхід системи надходить лог у вигляді «109.87.117.86 - - [16/Oct/2020:19:35:23 +0300] "GET /files/uploads/logos/softserve.png HTTP/1.1" 200 3771 "http://rabota.nure.ua/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:81.0) Gecko/20100101 Firefox/81.0" "-"».

А на виході системи отримуємо повідомлення на кшталт «16 жовтня 2020 року о 19-й годині 35 хвилин та 23 секунд за київським часом з IP-адреси 109.87.117.86 за допомогою програмного забезпечення Mozilla Firefox версії 81, яке встановлено на операційну систему Windows NT 10.0 x64 користувача, який підписаний як «Gecko»,

було здійснене успішне звернення до графічного файлу softserve.png розміром 3771 байт. Файл знаходиться на сайті rabota.nure.ua».

Завдяки такому представленню даних система може фільтрувати всі повідомлення та за певними критеріями, що може додати адміністратор, видавати оповіщення тривоги, наприклад, якщо певний користувач зробив 5 неуспішних спроб підключення до свого профілю.

2.2 Аналіз структури та механізмів виявлення та реагування на кіберінциденти Alienvault OSSIM

AlienVault OSSIM надає п'ять основних безпекових можливостей в єдиному рішенні SaaS, надаючи все необхідне для виявлення загроз, реагування на інциденти та управління комплаєнсом - все в одному вікні. З AlienVault OSSIM можна зосередитись на виявленні та реагуванні на загрози, а не на управлінні програмним забезпеченням. Еластичне, хмарне рішення для безпеки, AlienVault OSSIM може легко масштабуватися для задоволення ваших потреб у виявленні загроз, оскільки ваш гібридний хмарний простір змінюється та зростає.

Пошук активів:

- Пошук активів на основі API;
- Пошук активів у мережі;
- Пошук програмного забезпечення та сервісів.

Оцінювання уразливості:

- Сканування уразливості мережі;
- Сканування уразливості хмарних середовищ;
- Оцінювання інфраструктури хмар.

Виявлення вторгнень:

- Cloud IDS (Система виявлення вторгнень для хмарних середовищ);
- Network IDS (Система виявлення вторгнень для мереж);

- Host IDS (Система виявлення вторгнень для кінцевих точок);
- Файловий моніторинг цілісності.

Монторінг поведінки:

- Журнали доступу до активів;
- Журнали доступу до хмари (Azure Monitor, AWS: CloudTrail, CloudWatch, S3, ELB);
- Моніторинг потоків трафіку в VPC AWS;
- Журнали доступу до VMware ESXi.

SIEM:

- Кореляція подій;
- Управління журналами;
- Реагування на інциденти;
- Інтегровані дані AlienVault® Open Threat Exchange (OTX™);
- Зберігання вихідних журналів протягом 12 місяців.

Централізований моніторинг безпеки для ваших хмарних і локальних середовищ

AlienVault OSSIM надає вам потужні можливості виявлення загроз у ваших хмарних і локальних середовищах, допомагаючи усувати сліпі зони безпеки та зменшувати вплив тіньової IT. Навіть при міграції робочих навантажень і сервісів з центру обробки даних у хмару, ви можете бути впевнені в безперервному моніторингу безпеки.

AlienVault OSSIM здійснює моніторинг:

- Публічних хмар AWS і Microsoft Azure;
- Віртуальної локальної IT на VMware/Hyper-V;
- Фізичної IT-інфраструктури у вашому центрі обробки даних;
- Інших локальних об'єктів (наприклад, офісів, роздрібних магазинів тощо).

Автоматизоване управління відповідями

AlienVault OSSIM надає розширені правила оркестрації безпеки, які автоматизують дії та реакції відповідно до ваших потреб, що підвищує ефективність роботи. Ви можете:

- Зменшити рівень шуму за допомогою правил придушення: мінімізувати кількість помилкових спрацьовувань;
- Генерувати власні сповіщення: налаштовувати сповіщення на основі будь-якого параметра;
- Автоматично реагувати на події: встановлювати автоматичні дії за відповідними правилами;
- Створювати правила оркестрації для сторонніх програм: інтегрувати AlienVault OSSIM з іншими інструментами безпеки для розширених можливостей.

Потужний аналіз безпеки під рукою

AlienVault OSSIM пропонує інтуїтивно зрозумілий і гнучкий інтерфейс для пошуку та аналізу даних, пов'язаних із безпекою. З його допомогою ви можете:

- Шукати та аналізувати дані для виявлення загроз та розслідування інцидентів: знаходити необхідні дані серед даних активів, вразливостей і подій;
- Переходити між активами, вразливостями та даними подій: з легкістю орієнтуватися серед різних типів даних;
- Створювати та експортувати власні подання даних для звітів відповідності вимогам: генерувати зручні звіти для підтвердження відповідності різним стандартам.

Створено для хмари

На відміну від інших застарілих рішень безпеки, які були модифіковані для роботи в хмарі, AlienVault OSSIM є справді хмарною системою моніторингу безпеки. Вона використовує унікальні елементи безпеки інфраструктури публічної хмари. AlienVault OSSIM використовує прямі підключення до API хмари, щоб надати вам більш повний набір даних, більший контроль над безпекою вашої хмари та більш швидку видимість вашого хмарного середовища протягом хвилин після встановлення.

Розширений аналітичний двигун на основі графів

AlienVault OSSIM використовує новий підхід до кореляції подій SIEM, що робить аналіз безпеки швидшим, більш гнучким і більш ефективним, ніж будь-коли. Завдяки нашому унікальному підходу до кореляції на основі графів ви можете:

- Переглядати повну модель стану вашого середовища в будь-який момент часу та порівнювати різні періоди;
- Швидко і ефективно виконувати спеціальні запити до великих і складних наборів даних;
- Покращувати кореляцію за допомогою ключових з'єднань між активами, користувачами та діями та змінами, що відбуваються між ними.

Розширена оркестрація безпеки з AlienApps

AlienVault OSSIM є високорозширюваною платформою, яка використовує AlienApps — інтеграції зі сторонніми інструментами безпеки та продуктивності - для розширення можливостей оркестрації безпеки. За допомогою AlienApps ви можете:

- Витягувати дані із сторонніх програм безпеки: інтегрувати дані з інших інструментів для більш цілісної карти безпеки;
- Візуалізувати зовнішні дані на інтуїтивно зрозумілих панелях: легко відслідковувати та аналізувати дані з різних джерел;
- Автоматично надсилати дії до сторонніх інструментів безпеки: реагувати на загрози за допомогою інших інструментів;
- Розширювати можливості за допомогою нових AlienApps: отримувати доступ до нових функцій і інтеграцій з розвитком платформи.

AlienVault OSSIM вже інтегровано з такими популярними програмами безпеки, як Cisco Umbrella і McAfee ePO, що дозволяє збирати дані і автоматично реагувати на загрози.

2.3 Основні компоненти та їх взаємодія в AlienVault OSSIM

OSSIM - це платформа програмного забезпечення для системи управління інформацією та подіями безпеки (SIEM), яка є вільною та відкритою, розробленою компанією AlienVault і заснованою на дистрибутиві Debian 64-бітного Linux. У OSSIM існують чотири основні компоненти:

1. Сенсор (Sensor).
2. Сервер (Server).
3. Фреймворк (Framework).
4. База даних (Database).

Ви можете встановити ці компоненти на одному фізичному комп'ютері (стандартна установка), на одній віртуальній машині, на різних віртуальних та/або фізичних машинах, залежно від розміру та конфігурації мережі, яку ви плануєте моніторити.

Для відносно невеликої мережі установка на одній машині, що є найпростішою конфігурацією, може бути правильним рішенням. Для більших мереж рекомендується встановлювати Сенсор і Базу даних окремо. На малюнку 1 показано архітектуру OSSIM.

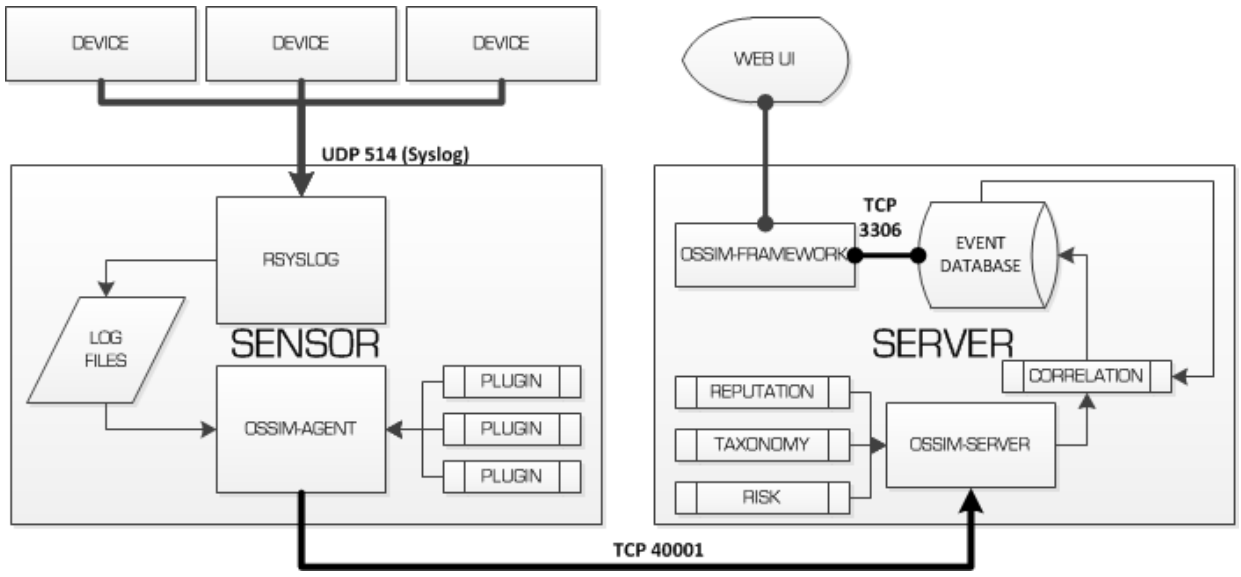


Рис. 2.3. Аріхтектура OSSIM [4]

Сенсор:

Розгортаються по всій мережі для збору та нормалізації інформації з будь-яких пристроїв у вашому мережевому середовищі, які ви хочете управляти за допомогою AlienVault OSSIM. Доступний широкий спектр плагінів для обробки сирих логів та даних з різних типів пристроїв, таких як брандмауери, роутери та сервери хостів.

Сенсор має два основних компонента:

1. Служба rsyslog, яка слухає на TCP/UDP-порту 514, отримує логи від мережевих пристроїв і зберігає їх локально відповідно до конфігурації.

2. Ossim-agent, використовуючи серію модулів, називаних плагінами, один для кожного типу логів, виконує аналіз та нормалізацію логів і відправляє їх на компонент Сервер.

Плагіни поділяються на два типи: детектори, які виявляють аномалії та можливі атаки (наприклад, Snort, P0f, Arpwatch), та монітори для відстеження стану мережі (наприклад, Ntop і Nagios).

Сервер:

Збирає та корелює інформацію, яку збирають AlienVault OSSIM Sensors. (Це є можливість SIEM для AlienVault OSSIM.) Надає єдиний інтерфейс управління, звітності та адміністрування через веб-інтерфейс користувача.

Сервер виконує основні функції SIEM: агрегацію, оцінку ризику та кореляцію подій, які надходять від сенсора через TCP-порт 40001. Сервер також відправляє інформацію про події в базу даних для зберігання.

Фреймворк:

Фреймворк підключає та керує компонентами OSSIM та включеними інструментами безпеки, і надає веб-інтерфейс адміністрування системи. Це компонент, який потребує найменше апаратних ресурсів і, як правило, встановлюється разом із компонентом Сервер.

База даних:

База даних - це екземпляр сервера MySQL, який зберігає дані про події та конфігурацію системи.

Функціональності

Нижче подано короткий опис основних функцій та можливостей OSSIM щодо збору, аналізу та кореляції логів, а також основних інструментів, включених у систему для моніторингу безпеки мережі.

Збір та нормалізація логів:

Агент AlienVault - це легкий агент для кінцевих точок, що базується на osquery, провідній відкритій операційній системі (ОС) для Microsoft Windows, Apple macOS та Linux. Він дозволяє виявлення та моніторинг кінцевих точок з централізованим управлінням, сприяючи повному та ефективному виявленню загроз, детектуванню та відповідності.

Агент AlienVault легко встановлюється на вашому хості та кінцевих точках і має невеликий слід. Встановлений агент забезпечує постійний моніторинг безпеки кінцевих точок, що дозволяє AlienVault OSSIM швидко виявляти загрози на вашому основному активі без часомістких налаштувань та завдань налаштування, необхідних для впровадження та інтеграції інструменту сторонньої сторони.

Ідентифікатори агента

Агент AlienVault взаємодіє через зашифрований канал для відправлення даних безпосередньо до служби AlienVault OSSIM, обходячи датчик AlienVault OSSIM, і буферизує дані локально, коли з'єднання з AlienVault OSSIM недоступне. Агенти (OS)se використовують два ідентифікатори унікальних універсальних ідентифікаторів (UUID) для взаємодії з AlienVault OSSIM: ідентифікатор хоста UUID та ідентифікатор активу UUID. Розуміння двох ідентифікаторів агента AlienVault є важливим при розгортанні агентів у віртуальних машинах (VM). Див. Ідентифікатори агента AlienVault для отримання додаткової інформації.

Збір даних агента

Кожний агент AlienVault повинен бути пов'язаний з активом у AlienVault OSSIM для можливості збору логів, який повинен відповідати системі хосту, де він розгорнутий. Коли ця асоціація встановлена, детальна інформація доступна на сторінці Деталі активу. На цій сторінці ви можете переглядати кількість подій, пов'язаних з агентом, а також споживання даних агентом протягом фіксованого періоду часу.

Коли агент зареєстрований і пов'язаний з активом, профіль конфігурації агента визначає запити та інтервали, які AlienVault OSSIM використовує для збору логів з системи хосту.

Інформацію про стан всіх агентів, зареєстрованих у вашому середовищі AlienVault OSSIM, включаючи позначку, що агент в даний момент відправляє дані, можна переглядати на панелі інструментів агента AlienVault. Див. Інформацію на Панелі інструментів агента AlienVault для отримання додаткової інформації.

Кешування даних агента

AT&T Cybersecurity покращила буферний реєстратор osquery для ефективного зберігання даних, якщо відбудеться збій зв'язку з AlienVault OSSIM. На основі частоти подій, що генеруються на кінцевій точці, агент AlienVault записує ці події в партійні файли. Коли виникає помилка зв'язку з AlienVault OSSIM, ці файли зберігаються в osquery3.db/z_cached_logs у робочому каталозі агента. Агент намагається відправити файли після періоду резервування, а водночас продовжує додавати нові файли для нових подій, якщо зв'язок не відновлено. У звичайних умовах кеш файлів не повинен перевищувати 5 ГБ дискового простору. Після відновлення зв'язку агент працює зі стопою файлів в порядку їх створення. Якщо досягнуто межі кешування, агент видає попередження і припиняє запис даних у кеш на диск, після чого нові події не фіксуються. Вам може бути потрібно видалити деякі або всі файли, щоб дозволити агенту зафіксувати і кешувати нові події, поки не відновиться зв'язок із AlienVault OSSIM. Час, необхідний для досягнення межі кешування, залежить від активності на кінцевій точці та обсягу вмісту в кожній події.

Оновлення агента

Коли новий агент реєструється у вашій службі AlienVault OSSIM, система перевіряє його версію і відображає її під асоційованим активом. Ви можете оновити агент вручну або використовувати функцію автоматичного оновлення агента, яка за замовчуванням вимкнена. Обидва методи оновлення виконуються за допомогою скрипта агента AlienVault. Див. Оновлення агента AlienVault на сторінці Оголошень продукту AlienVault OSSIM, щоб дізнатися останню версію агента та поліпшення.

Ви можете збирати логи з пристроїв у своїй мережі двома способами:

1. Встановити агент програмного забезпечення (наприклад, Snare або SysLogAgent) на джерело і налаштувати його на читання певних типів логів та відсилання їх на компонент Сенсор;

2. Налаштувати джерело на відсилання логів за запитом від відповідних плагінів Сенсора (наприклад, через WMI для машин з операційною системою Windows). Після того, як Сенсор реєструє логи, агент OSSIM виконує аналіз та перетворення їх в єдиний формат (нормалізація). Кожен лог представляє собою подію, яку буде відправлено на сервер для аналізу. [4]

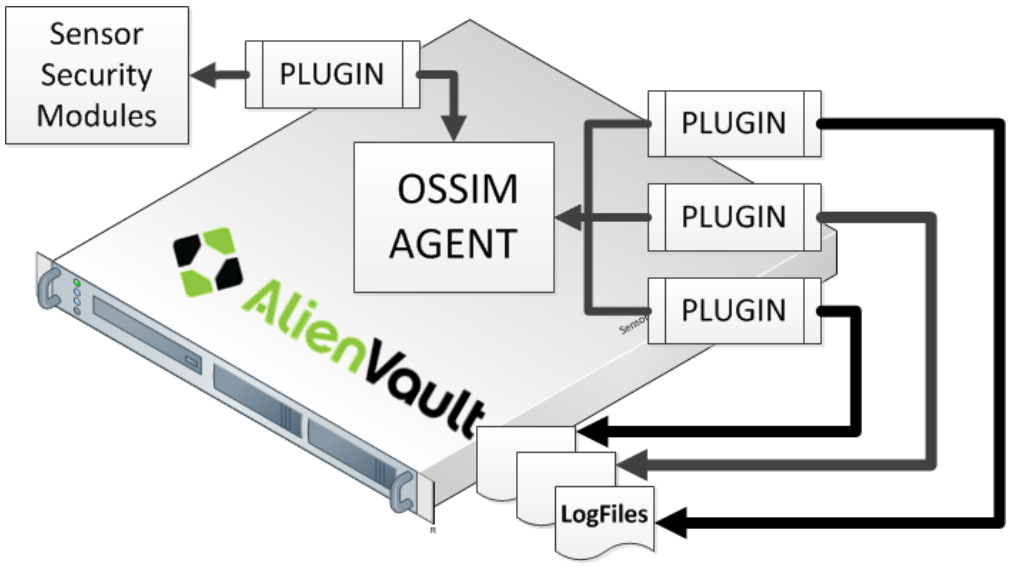


Рис. 2.4. Збір та нормалізація логів [4]

Пріоритетизація подій та оцінка ризику:

Процес пріоритетизації включає надання пріоритетних значень записаним подіям, що виконується компонентом Сервер. Це залежить від структури мережі і вимагає визначення політик безпеки та інвентаризації інформаційних активів в мережі, що можна керувати в панелі веб-адміністрування. Процес встановлює пріоритет події на основі машини, що її згенерувала, та типу події, до якого вона належить.

Оцінка ризику подій обчислюється в реальному часі і базується на трьох основних факторах:

1. Значення або рівень важливості машини, що згенерувала подію;
2. Тип загрози, яку представляє подія;
3. Ймовірність того, що ця подія станеться.

Формула для обчислення ризику виглядає наступним чином Ризик = значення * (надійність * Пріоритет / 25). [4]

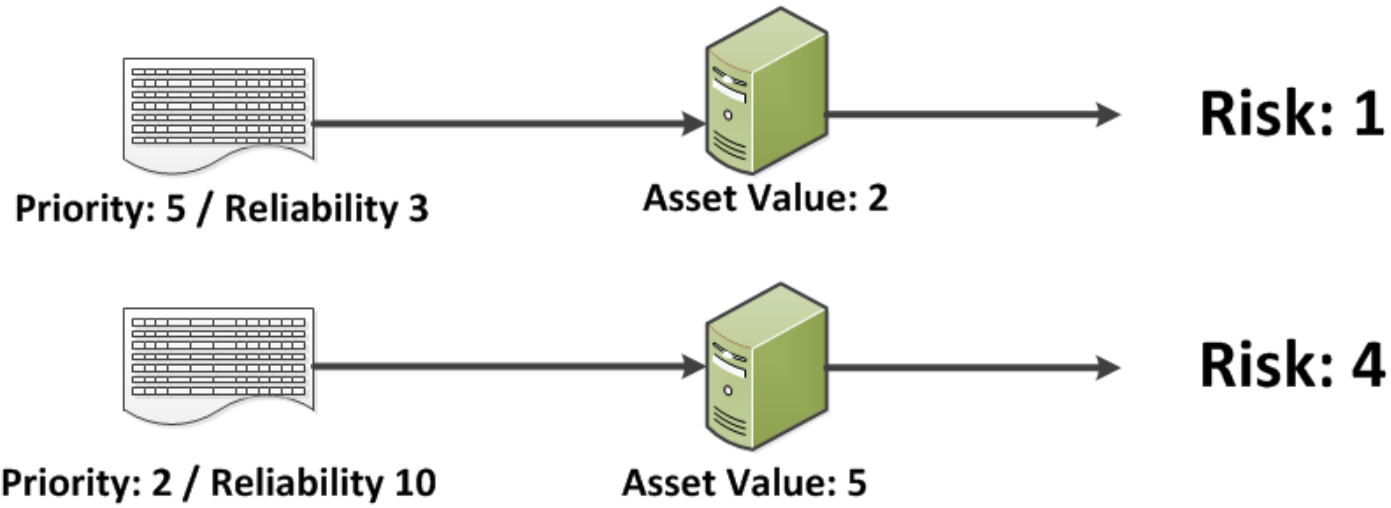


Рис. 2.5. Як розрахувати ризик, пов'язаний з подією [4]

Аналіз та кореляція подій:

Кореляція подій в сутності встановлює зв'язки між подіями для досягнення комплексного уявлення про безпеку мережі та виявлення можливих атак чи аномалій.

Процес кореляції виконується двома методами:

1. Кореляція за допомогою послідовності подій, використовуючи директиви, які складаються з правил, які встановлюють зв'язки між подіями та шаблонами відомих атак. Цей метод подібний до використання Snort для виявлення вторгнень (виявлення на основі сигнатур).

2. Кореляція за допомогою евристичних алгоритмів може виявляти ненормальні ситуації, які не виявляються попередніми правилами і можуть або не можуть бути атаками (виявлення аномалій).

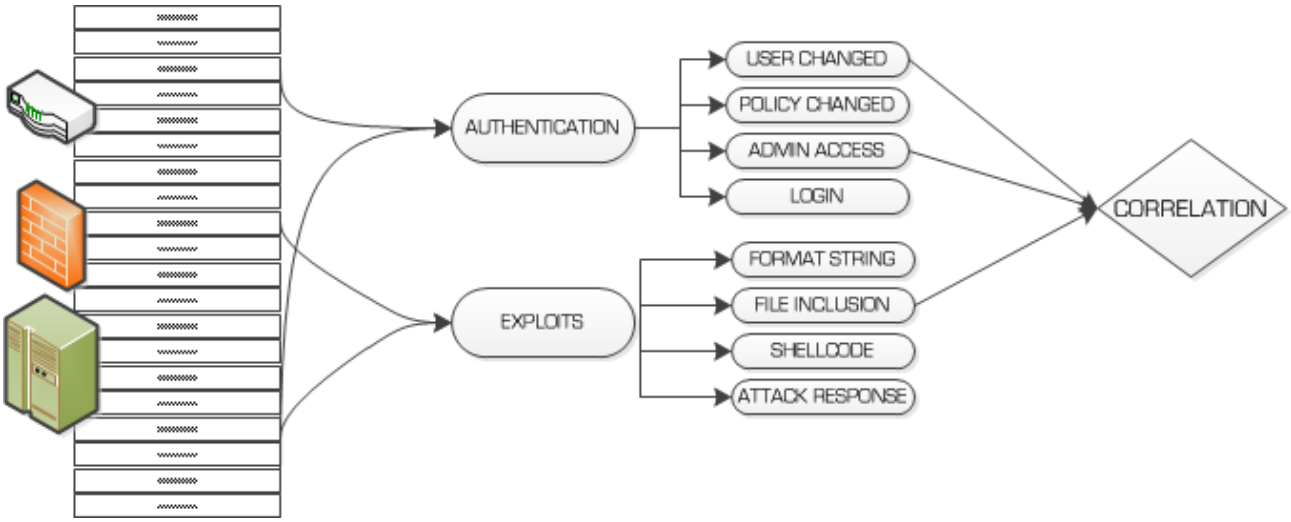


Рис. 2.6. Приклад аналізу та кореляції подій [4]

Директиви розташовані у файлі /etc/ossim/server/directives.xml. Директиви вказуються в форматі XML за допомогою тегів, таких як Id, Name, Priority, Type, Reliability, Occurrence, Timeout, Source, Destination, Source port, destination port, protocol, PluginSid та Sensor.

Надійність - це міра ймовірності того, що розглянута подія дійсно представляє атаку, на яку вказує директива, і, як правило, базується на кількості випадків події.

Директива встановлює значення надійності рівним 3 (30% ймовірність), коли кількість випадків події, виявленої сенсором (помилка аутентифікації SSH), рівна 1, потім збільшує його на 1 при третьому випадку події, на 2 при п'ятому випадку та ще на 2 при десятому, досягаючи тим самим надійності 8 (80% ймовірність), коли спроби неправильної аутентифікації становлять 10.

OSSIM також має можливість корелювати різні типи логів, що генеруються різними плагінами (перехресна кореляція). Перехресна кореляція дозволяє змінювати надійність події та оцінку ризику. Наприклад, припустимо, що Nessus або OpenVAS виявили вразливість на сервері. Якщо Snort виявляє подію, яка вказує на можливу атаку на цей сервер, рівень ризику, пов'язаний з цією подією, збільшується.

Генерація сигналів тривог та виконання дій у відповідь:

Директиви можуть створювати сигнали тривог, які можуть бути згенеровані однією подією або конкретною послідовністю подій за певних умов. Сигнали тривог можуть бути відображені в веб-панелі адміністрування під пунктом меню "Інциденти→Сигнали тривог".

Крім того, сигнали тривог можуть активувати дії у відповідь, такі як відсилання сповіщення по електронній пошті системному адміністратору і/або виконання відповідних скриптів.

3. РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ ALIENVAULT OSSIM

3.1 Алгоритм аналізу мережі та пошук загроз за допомогою AlienVault OSSIM

Виявлення атак брутфорс, здійснених за допомогою різних протоколів

Брутфорс – це атака, при якій зловмисник намагається увійти в систему, не знаючи імені користувача та його пароля. Можна захистити себе від подібної небезпеки за допомогою різних типів SIEM-інструментів, одним з яких є AlienVault. Варто розглянути практичний приклад.

Зливмисник планує виконати атаку брутфорс за допомогою різних протоколів. Для здійснення атаки на основі протоколу SSH зливмисник запустить машину Kali та введе наступну команду: hydra -L user.txt -P passwd.txt 192.168.0.150 ssh

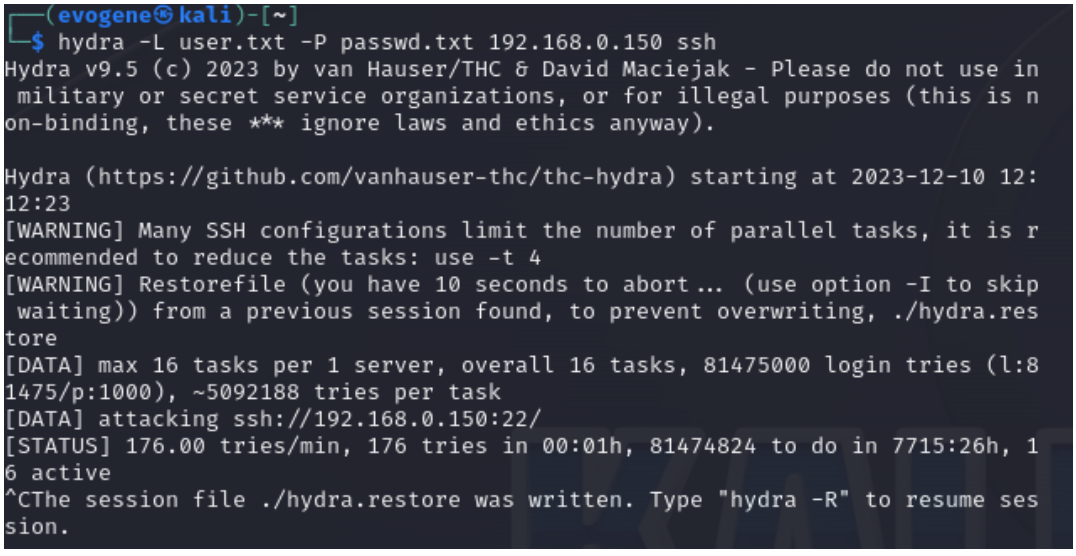


Рис 3.1. Запуск брутфорс атаки по протоколу SSH

Тепер необхідно розглянути результат. Програма виявила кілька неуспішних спроб входу в систему.

SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51566	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51606	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51546	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51506	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51556	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51520	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51484	0.0.0.0:22	2->2	LOW (0)	
SSHd: Failed password	2023-12-10 12:18:27	alienvault	N/A	Host-192-168-0-103:51494	0.0.0.0:22	2->2	LOW (0)	
AlienVault HIDS: SSHD brute force trying to get access to the system.	2023-12-10 12:18:25	alienvault	N/A	Host-192-168-0-103:51530	0.0.0.0	2->2	LOW (0)	
AlienVault HIDS: Multiple failed logins in a small period of time.	2023-12-10 12:18:25	alienvault	N/A	Host-192-168-0-103	0.0.0.0	2->2	LOW (0)	
AlienVault HIDS: Attempt to login using a non-existent user	2023-12-10 12:18:25	alienvault	N/A	Host-192-168-0-103:51578	0.0.0.0	2->2	LOW (0)	
AlienVault HIDS: Attempt to login using a non-existent user	2023-12-10 12:18:25	alienvault	N/A	Host-192-168-0-103:51502	0.0.0.0	2->2	LOW (0)	
AlienVault HIDS: Attempt to login using a non-existent user	2023-12-10 12:18:25	alienvault	N/A	Host-192-168-0-103:51608	0.0.0.0	2->2	LOW (0)	

Рис 3.2. Реагування AlienVault OSSIM на атаку

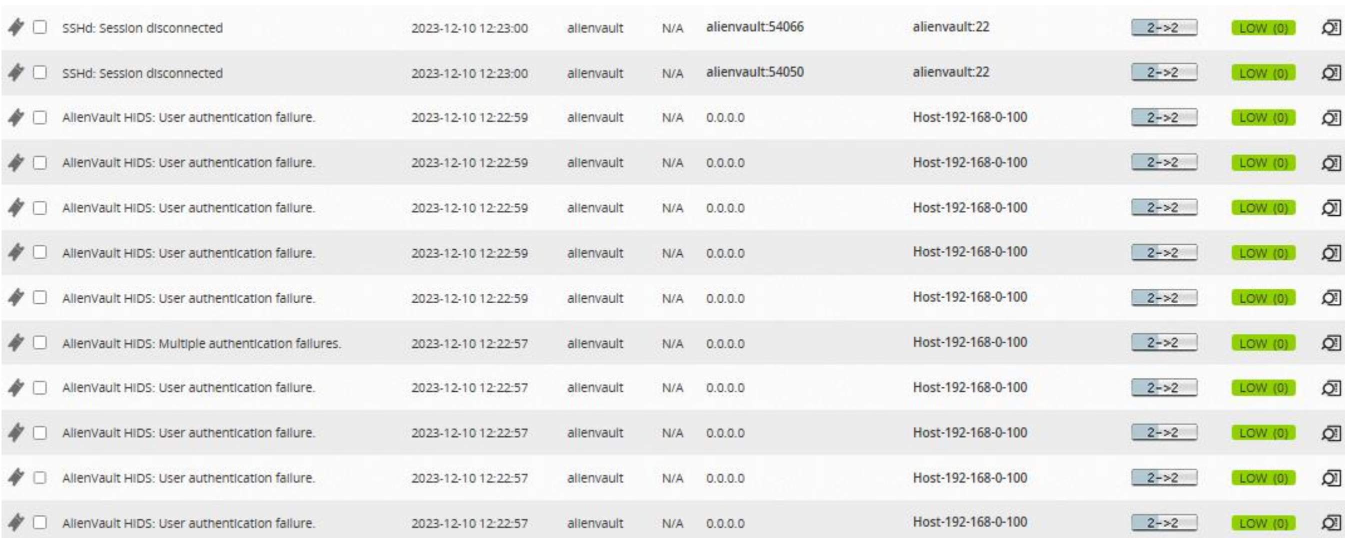
Зливмисник виконає ще одну атаку брутфорс, використовуючи протокол SSH, щоб переконатися, що інструмент може виявити атаку на маршрутизатор Mikrotik в мережі. Таким чином, введемо наступну команду для здійснення нападу: hydra -L user.txt -P passwd.txt 192.168.0.100 ssh

```
┌──(evogene㉿kali)-[~]
└─$ hydra -L user.txt -P passwd.txt 192.168.0.100 ssh -I
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-10 12:22:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 81475000 login tries (l:81475/p:1000), ~5092188 tries per task
[DATA] attacking ssh://192.168.0.100:22/
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Рис 3.3. Запуск брутфорс атаки по протоколу SSH на Mikrotik

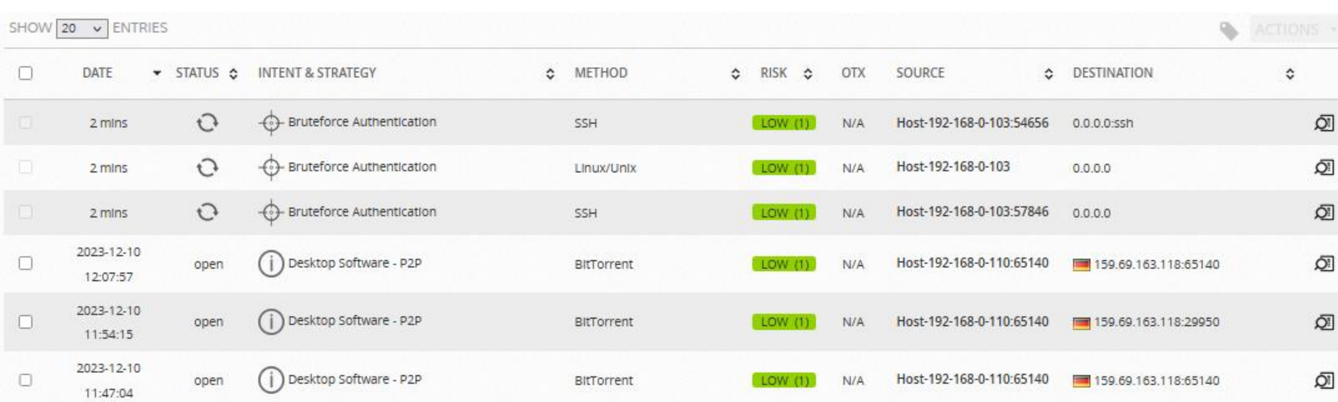
Потрібно перевірити записи в журналі. Програма також виявила кілька неуспішних спроб входу в систему з даними хоста чи джерела. Це досить ефективний спосіб уникнути атак брутфорс.



SSHd: Session disconnected	2023-12-10 12:23:00	alienvault	N/A	alienvault:54066	alienvault:22	2->2	LOW (0)
SSHd: Session disconnected	2023-12-10 12:23:00	alienvault	N/A	alienvault:54050	alienvault:22	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:59	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:59	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:59	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:59	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:59	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: Multiple authentication failures.	2023-12-10 12:22:57	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:57	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:57	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:57	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)
AlienVault HIDS: User authentication failure.	2023-12-10 12:22:57	alienvault	N/A	0.0.0.0	Host-192-168-0-100	2->2	LOW (0)

Рис 3.4. Реагування AlienVault OSSIM на атаку

Крім того, зливмисник здійснив кілька атак у мережі. AlienVault виявив усі загрози та швидко згенерував повідомлення про небезпеку в розділі «Alarms».



SHOW 20 ENTRIES ACTIONS

DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
2 mins		Bruteforce Authentication	SSH	LOW (1)	N/A	Host-192-168-0-103:54656	0.0.0.0:ssh
2 mins		Bruteforce Authentication	Linux/Unix	LOW (1)	N/A	Host-192-168-0-103	0.0.0.0
2 mins		Bruteforce Authentication	SSH	LOW (1)	N/A	Host-192-168-0-103:57846	0.0.0.0
2023-12-10 12:07:57	open	Desktop Software - P2P	BitTorrent	LOW (1)	N/A	Host-192-168-0-110:65140	159.69.163.118:65140
2023-12-10 11:54:15	open	Desktop Software - P2P	BitTorrent	LOW (1)	N/A	Host-192-168-0-110:65140	159.69.163.118:29950
2023-12-10 11:47:04	open	Desktop Software - P2P	BitTorrent	LOW (1)	N/A	Host-192-168-0-110:65140	159.69.163.118:65140

Рис 3.5. Ідентифікація загроз в AlienVault OSSIM

Далі потрібно перевірити деталі інциденту: який тип атаки був здійснений і як саме це було зроблено. Інформативний звіт можна переглянути, обравши пункт «View Details».

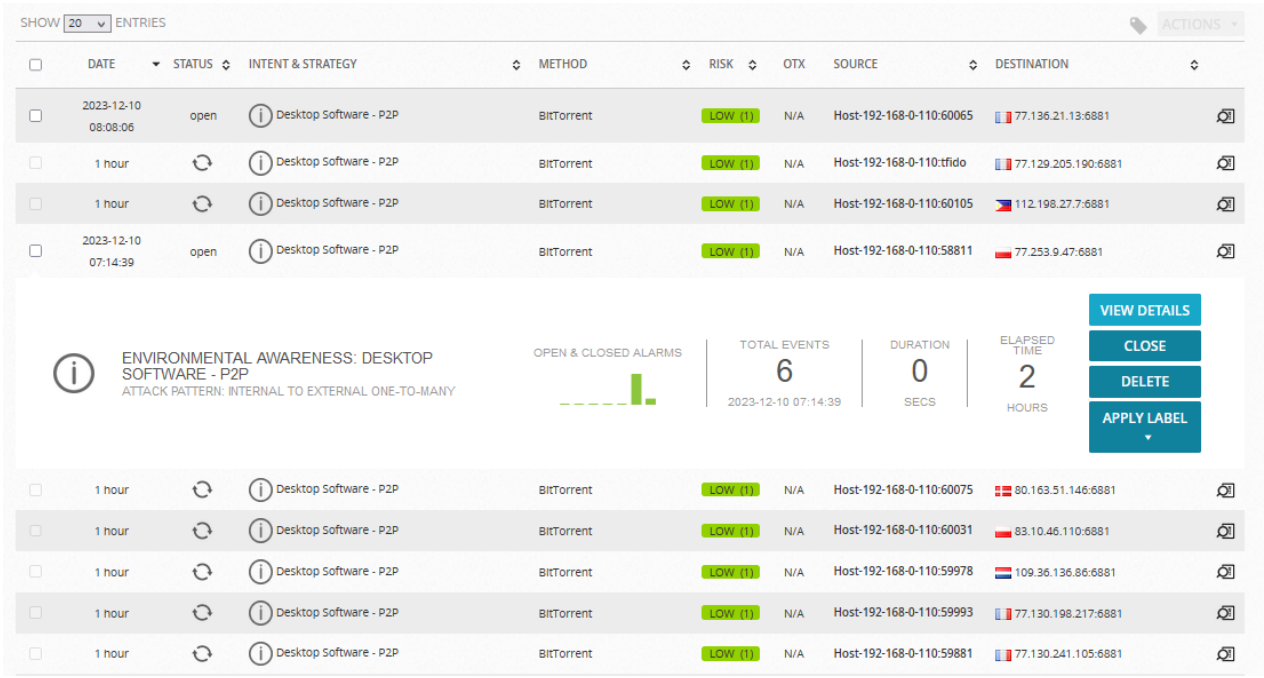


Рис 3.6. Інформативний звіт атаки в AlienVault OSSIM

Alerts Attack за допомогою Tickets

Tickets можуть забезпечити доступ до системи управління пристроями OSSIM. Це корисно для відстеження процесів, пов'язаних із виявленням так званих «сигналів тривоги», таких як вразливості, знайдені в системі або додатках, чи інші помилки, які можуть виникнути.

У даному випадку OSSIM згенерував кілька Tickets після автоматичного сканування вразливостей. Адміністратор може переглядати загальний список Tickets за замовчуванням у веб-інтерфейсі OSSIM. Крім того, є можливіть натискати кнопку «Create», щоб створити новий Ticket певного типу чи категорії.

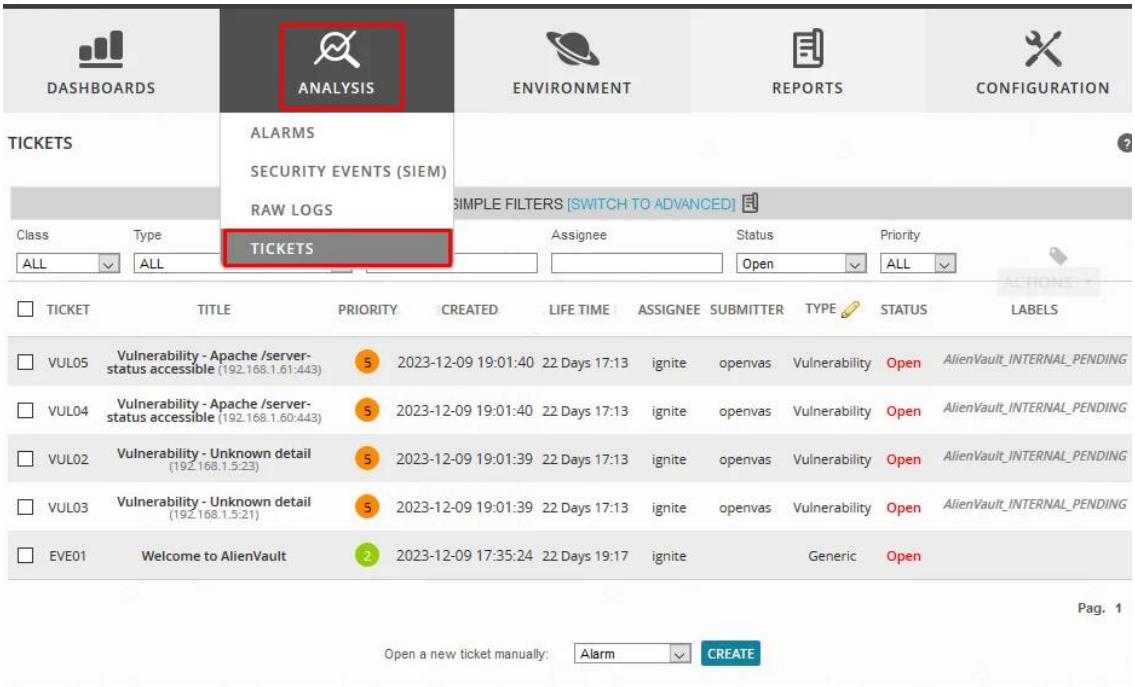


Рис 3.7. Генерування тікетів в AlienVault OSSIM

У розділі «Filters» у верхній частині сторінки можна встановлювати критерії для фільтрації результатів пошуку Tickets. Також можна вибрати додаткові фільтри, натиснувши кнопку «Switch to Advanced».

У загальному списку Tickets можна натискати на конкретний білет, щоб відкрити його та переглядати всю інформацію про нього на новій сторінці. У цьому вікні деталей білета можна виконувати різні дії, такі як редагування полів, призначення білета, додавання приміток і вкладень, а також змінювати статус і пріоритет в залежності від того, який метод чи процес потрібно використовувати для вирішення проблеми.

Аналіз трафіку

Ця опція дозволяє контролювати та керуваьт віддаленим захопленням трафіку за допомогою сенсора OSSIM. Є кілька доступних параметрів при захопленні трафіку: час очікування; розмір фільтруючого пакета; ім'я сенсора; джерело та призначення пакетів. Слід перевірити, як AlienVault виконує аналіз трафіку.

Щоб виконати захоплення трафіку, слід перейти за наступним шляхом: «Environment > Traffic Capture» та встановити фільтри відповідно до потреб. У нашому випадку - час очікування у 90 секунд і джерело, конкретна IP адреса.

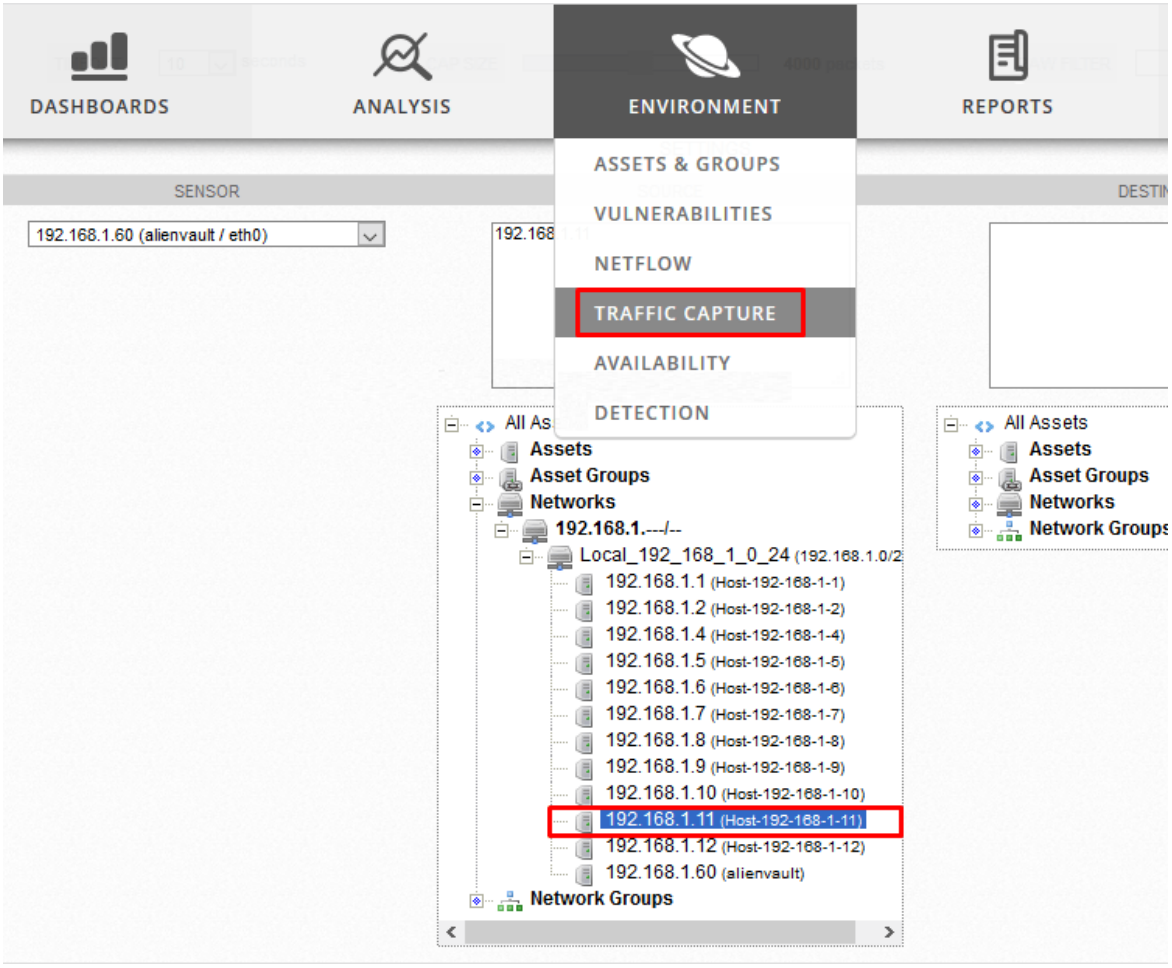


Рис 3.8. Інтерфейс Traffic Capture в AlienVault OSSIM

Після запуску захоплення трафіку програма зберігає результати, які можна переглянути. Також є можливість зберегти звіт у форматі PCAP. Його можна переглянути, якщо натиснути на потрібний значок.

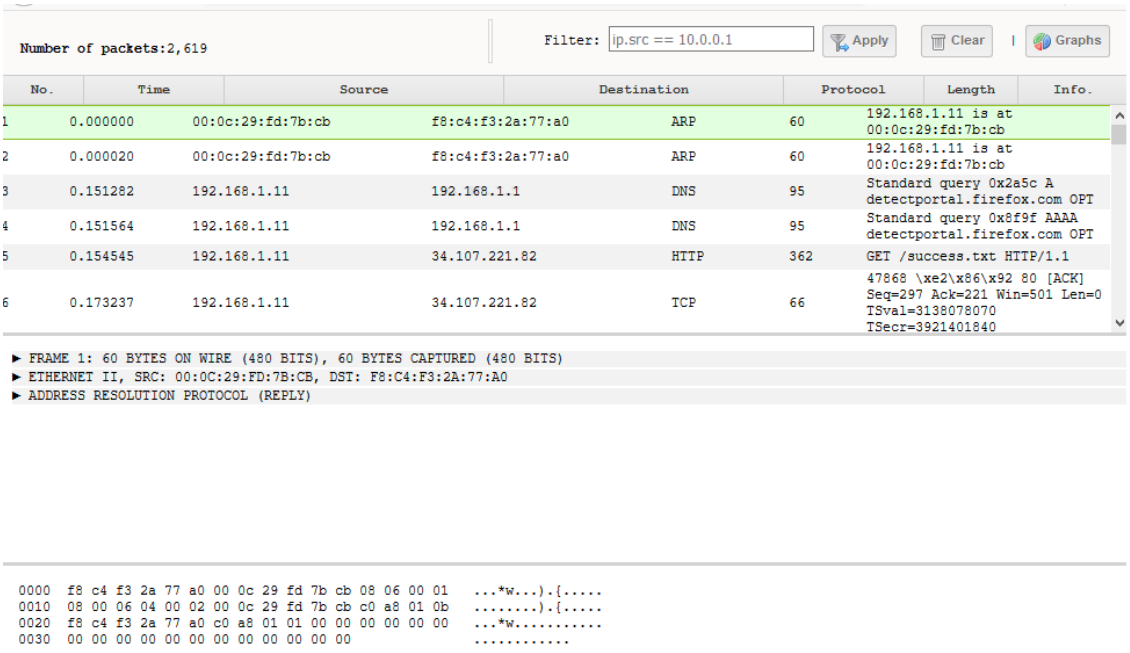


Рис 3.9. Звіт у форматі PCAP в AlienVault OSSIM

Отже, програма захоплює різні типи пакетів, таких як UDP чи TCP. Програма дає змогу адміністраторам контролювати всю мережу за допомогою цієї опції.

Стан розгортання

Потрібно перейти за шляхом: «Configuration > Deployment». Цей розділ надає інформацію про стан та ресурси різних компонентів OSSIM. Тут також є опції для їх налаштування. Серед цих компонентів можна виділити наступні: сенсори AlienVault; сервери пристроїв OSSIM; реєстратори пристроїв OSSIM. Отже, в програмі можна переглядати та змінювати параметри конфігурації існуючих компонентів, як показано на зображенні нижче.

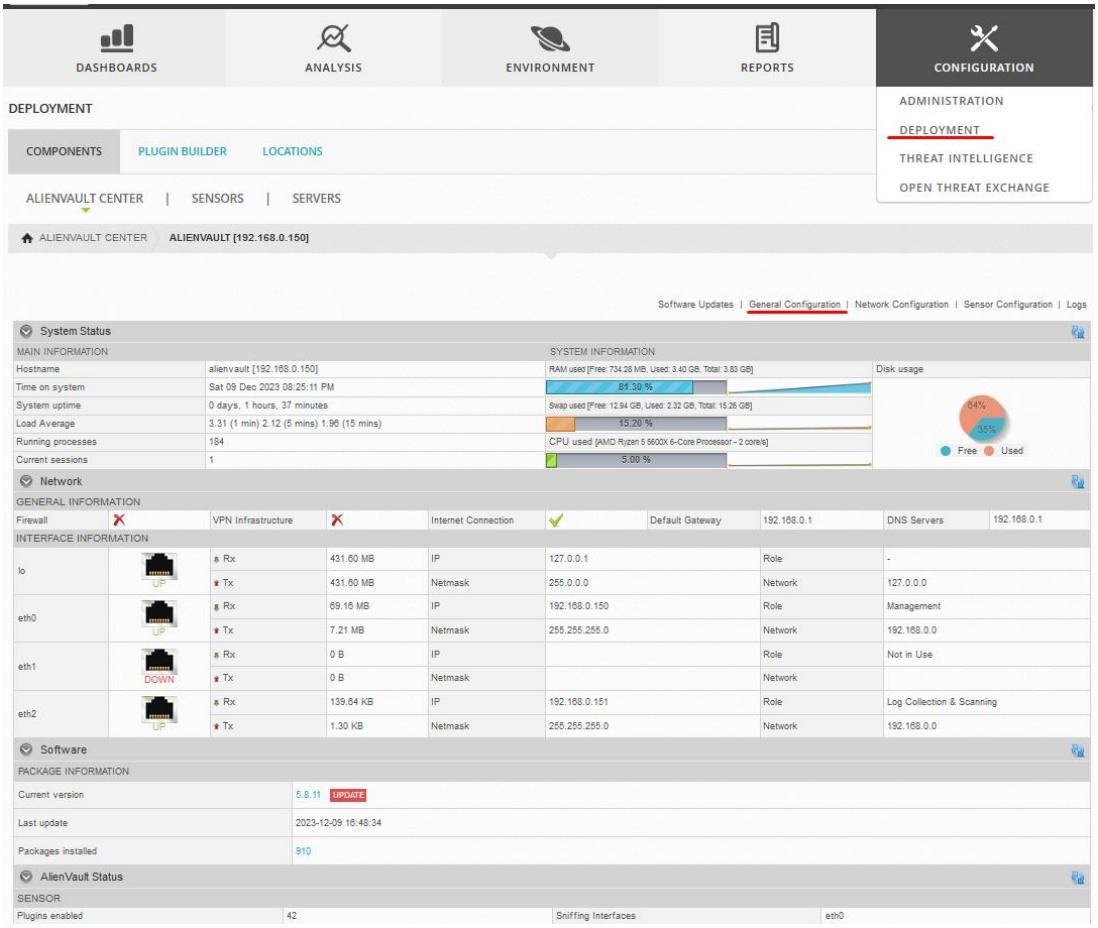


Рис 3.10. Інтерфейс стану системи та компонентів в AlienVault OSSIM

OTX: Open Threat Exchange

Open Threat Exchange або OTX – це відкрита мережа для обміну інформацією про проблеми та загрози безпеки. Програма забезпечує доступ до інформації в реальному часі. Це дає можливість вчитися на помилках інших людей, які вже пережили атаки зловмисників. AT&T AlienLabs та інші дослідники безпеки постійно аналізують та вивчають атаки, повідомляючи учасникам мережі про такі загрози, як шкідливі програми, ботнети та фішингові компанії.

Необхідно перейти за шляхом: «Configuration > Open Threat Exchange». Та відкриється наступне вікно:

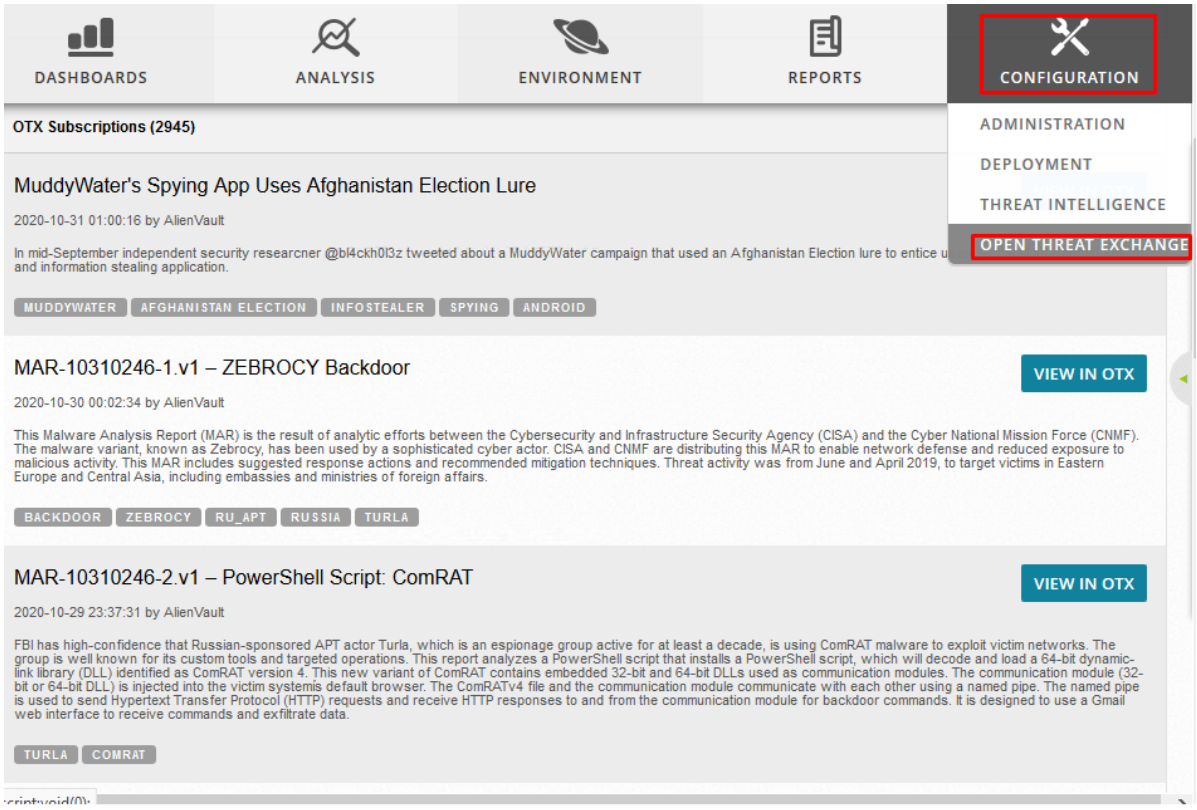


Рис 3.11. Інтерфейс Open Threat Exchange в AlienVault OSSIM

Індикатори компрометації (IoCs)

Пошук загроз зазвичай розпочинається з аналізу середовища, яке необхідно захистити. Спеціалісти у сфері безпеки також вивчають інші джерела, пов'язані з роботою мережі, щоб постулювати потенційну загрозу. Після цього вони шукають індикатори компрометації (IOCs), зберігаючи їх у криміналістичних "артефактах". Саме це допомагає ідентифікувати небезпечні активності, які в подальшому можуть стати справжнім нападом. Ці артефакти представляють собою біти даних з журналів сервера, мережевого трафіку та його конфігурацій. Вони допомагають фахівцям у сфері безпеки визначити, чи були здійснені підозрілі дії. Є кілька видів артефактів:

1. Мережеві артефакти (моніторинг портів інтернет-систем, що прослуховують). Фахівці можуть відстежувати трафік, а також переглядати записи

пакетних сеансів у пошуках незвичайного вихідного трафіку, аномальної карти зв'язків, нерегулярних обсягів вхідних або вихідних даних;

2. Артефакти на основі хоста. Зміни у файлових системах та реєстрі Windows – це ті два місця, де фахівці з безпеки можуть знайти аномальні налаштування та шкідливий вміст. Сканування значень реєстру та моніторинг змін, внесених у файлові системи, – це стандартна діяльність у пошуку загроз;

3. Артефакти на основі аутентифікації. Моніторинг або перевірка входу (або спроб входу) привілейованих облікових записів на кінцевих точках, серверах та службах може бути корисною для фахівця з безпеки. Це допоможе йому йти слідом, залишеним зловмисником, щоб визначити, які облікові записи були скомпрометовані.

Також можна здійснити пошук загроз за допомогою OTX IOCs:

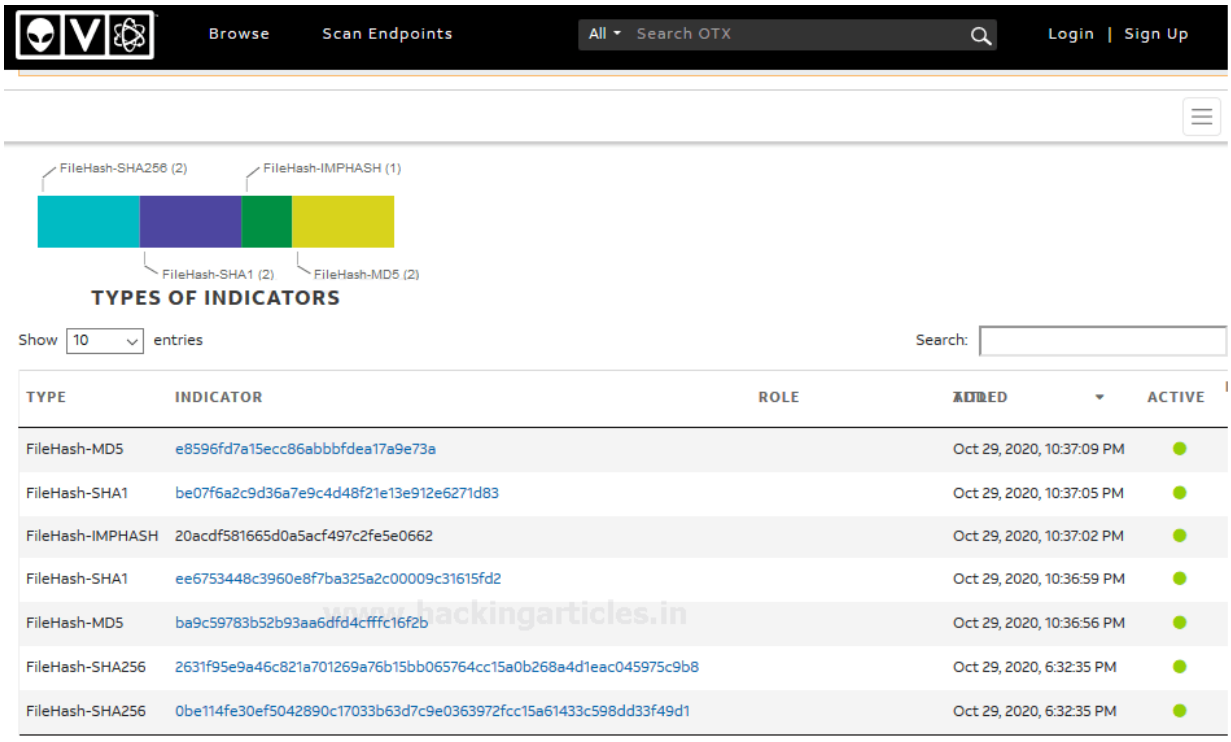


Рис 3.12. Пошук загроз за допомогою OTX AlienVault

Шлях, подоланий під час пошуку загроз, можна оцінити лише за знайденими уразливостями та небезпеками. Наприклад, виявлення аномального вихідного мережевого трафіку змусило б фахівця з безпеки уважніше придивитися до кінцевої точки, яка транслює цей трафік. Все залежить від конкретної проблеми, яка вирішується в даний момент.

3.2 Алгоритм налаштування розсилки повідомлень та політик тригерів у Alienvault OSSIM

Щоб налаштувати отримання електронних листів від AlienVault OSSIM. Наприклад, якщо потрібно отримувати лист, коли з'являється тривога, можна створити політику для надсилання листа.

AlienVault OSSIM використовує Postfix, відкритий поштовий агент (MTA), як сервер простого протоколу передачі пошти (SMTP) для вихідних повідомлень. Стандартні налаштування SMTP-сервера AlienVault OSSIM

SMTP - 25 - Це номер порту, призначений для SMTP та використовується для пересилання поштових серверів.

TLS (протокол транспортного рівня) - 587 - Це номер порту за замовчуванням, який AlienVault OSSIM використовує для відправлення вихідних повідомлень. Підключення шифрується за допомогою команди STARTTLS.

AlienVault OSSIM також активує наступні властивості від Postfix:

smtp_sasl_auth_enable = yes

smtp_sasl_security_options = noanonymous

smtp_sasl_tls_security_options = noanonymous

Це означає, що AlienVault OSSIM активує аутентифікацію Simple Authentication and Security Layer (SASL) для SMTP, відхиляючи анонімну аутентифікацію. Налаштування пересилання поштового сервера.

Якщо потрібно отримувати електронні листи від AlienVault OSSIM, тоді не потрібно налаштовувати пересилання поштового сервера. Однак, якщо у компанії є власний поштовий сервер, яким хочуть продовжувати користуватися, можна налаштувати AlienVault OSSIM для маршрутизації листів через корпоративну поштову програму. Щоб уникнути того, щоб такі повідомлення потрапляли в папку спаму, потрібно додати AlienVault OSSIM як безпечного відправника для Office 365 або додати його до списку дозволених адрес електронної пошти для Gmail.

Щоб налаштувати пересилання поштового сервера в AlienVault OSSIM

Потрібно увійти до веб-інтерфейсу AlienVault OSSIM та перейти до Configuration > Deployment. У розділі AlienVault Components Information треба натиснути значок відомостей системи, яку потрібно змінити. На наступній сторінці клацніть General Configuration, розташований вище System Status.

У формі General Configuration необхідно вибрати Yes для Mail Server Relay.

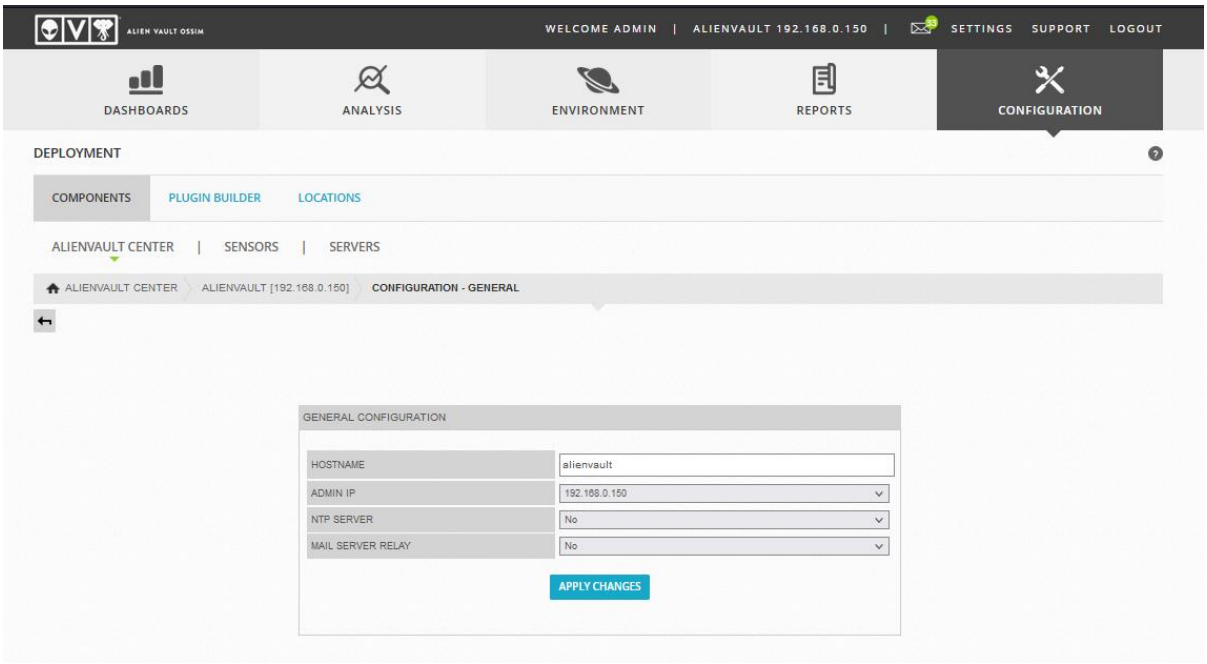


Рис 3.12. Інтерфейс підключення поштового серверу в AlienVault OSSIM

Це розгортає форму, в якій вказані нові поля.

Необхідно ввести IP-адресу сервера, ім'я користувача та пароль, які використовуються для поштового сервера, і номер порту в відповідні поля.

Поле IP-адреси сервера приймає дійсні IP-адреси або імена серверів.

Для Gmail: IP-адреса сервера: smtp.gmail.com Користувач: <your_email>@gmail.com або <your_user >@<your_domain>.tld, якщо < your_domain >.tld керується Google Professional Services Pass/Confirm Pass: <password> Порт: 587

Для Office 365: Якщо адміністратор Office 365 налаштував двоетапну перевірку для організації, можливо, доведеться створити пароль для додатка, який дозволить AlienVault OSSIM отримувати доступ до облікового запису Office 365. IP-адреса сервера: smtp.office365.com Користувач: < your_email > Pass/Confirm Pass: < password > Порт: 587

Для Exchange Server 2013: Перед тим як продовжувати, потрібно налаштувати з'єднання ретрансляції в Exchange Server 2013, щоб дозволити SMTP-ретрансляцію через службу Front End Transport. IP-адреса сервера: <IP-адреса вашого сервера Exchange Server 2013> Користувач: (залиште порожнім) Pass/Confirm Pass: (залиште порожнім) Порт: 25 (за замовчуванням) Клацніть Apply Changes. (Необов'язково) Якщо потрібно змінити адресу електронної пошти відправника (за замовчуванням - no-reply@alienvault.com), необхідно перейти до Configuration > Administration > Main.

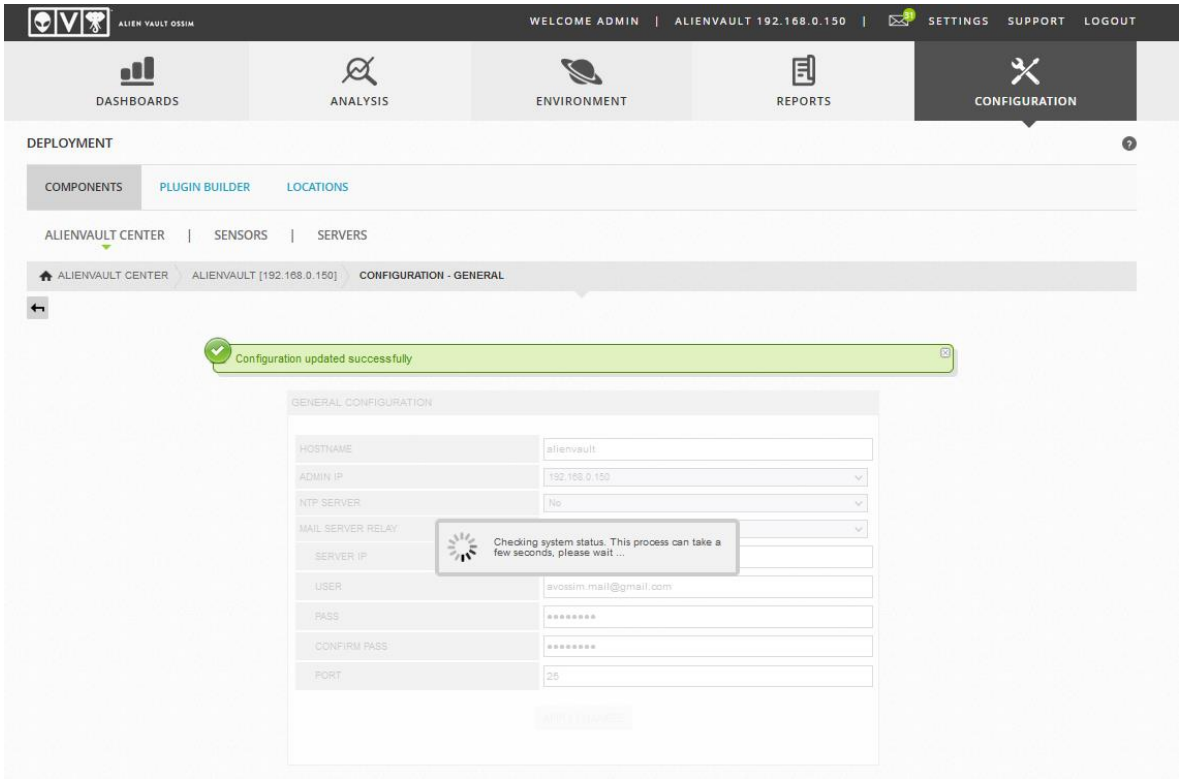


Рис 3.13. Успішне підключення поштового серверу в AlienVault OSSIM

Розгорніть USM Framework та оновіть адресу електронної пошти відправника для сповіщення.

AlienVault OSSIM використовує цю адресу електронної пошти для відправлення сповіщень у таких випадках: Розподіл звіту електронною поштою. AlienVault OSSIM повідомляє вас про відкриті тікети. AlienVault OSSIM створює тікет на основі виявленої уразливості. До існуючого тікета додається або змінюється коментар. Клацніть Update Configuration для застосування змін.

Створення політики для надсилання електронних листів, викликаних подіями

Для певних важливих подій є необхідність отримувати сповіщення, щоб негайно інформувати команду адміністраторів. У цьому пункті описано, як створити політику, яка дозволяє відсилати ці сповіщення. Створення дії для відправлення листа

Щоб створити умови політики для зовнішніх подій потрібно перейдти до Configuration > Threat Intelligence та клацнути на «ACTIONS». Натиснувши New.Необхідно заповнити всі обов'язкові поля. У полі «TYPE» виберіть Send an email message. Щоб відправити повідомлення кільком адресатам, ввівши адреси електронної пошти в полі «TO», розділені крапкою з комою(;). Клацніть «Save», щоб зберегти внесені зміни.

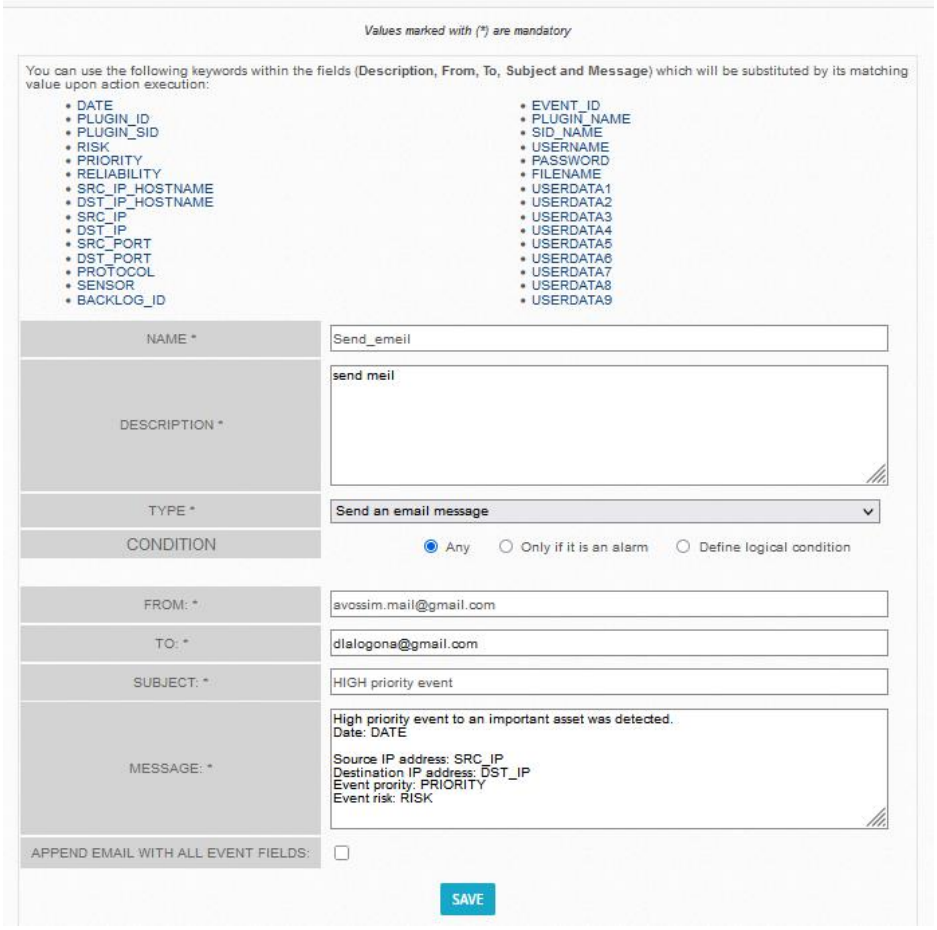


Рис 3.14. Налаштування політики в AlienVault OSSIM

Створення політики для ініціювання електронного листа. Для цього потрібно перейти до розділу Configuration (Конфігурація) > Threat Intelligence (Інтелект

безпеки) > Policy (Політика) > Default Policy Group (Група стандартних політик) та виберіть "New" (Створити нову).

У розділі Policy Conditions потрібно вибрати Source IP. Далі необхідно вибрати IP-адресу критичного сервера як актив для умови політики призначення. У даному випадку це підмережа 192.168.0.0/24.

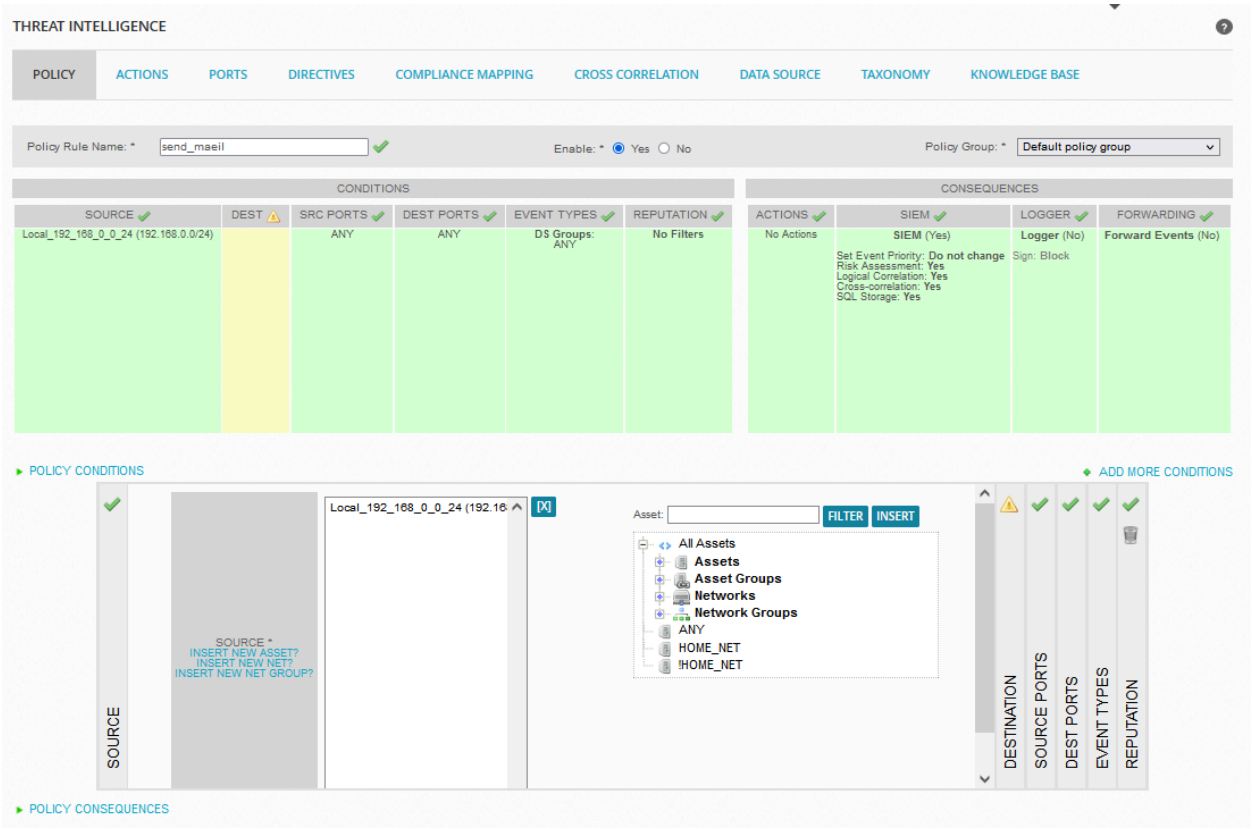


Рис 3.15. Налаштування умов політики в AlienVault OSSIM

Далі потрібно перейти до "Add More Conditions" і виберіть "Reputation" як умову політики.

Змініть значення «Reputation Parameters» наступним чином:

- Activity — Виберіть "Malicious Host".
- Priority — Виберіть > 4.
- Reliability — Виберіть > 8.

- Direction — Виберіть "Destination", оскільки потрібно виявити будь-які атаки на сервер з IP-адресою, яка використовується як умова.

Далі потрібно натиснути "Add New".

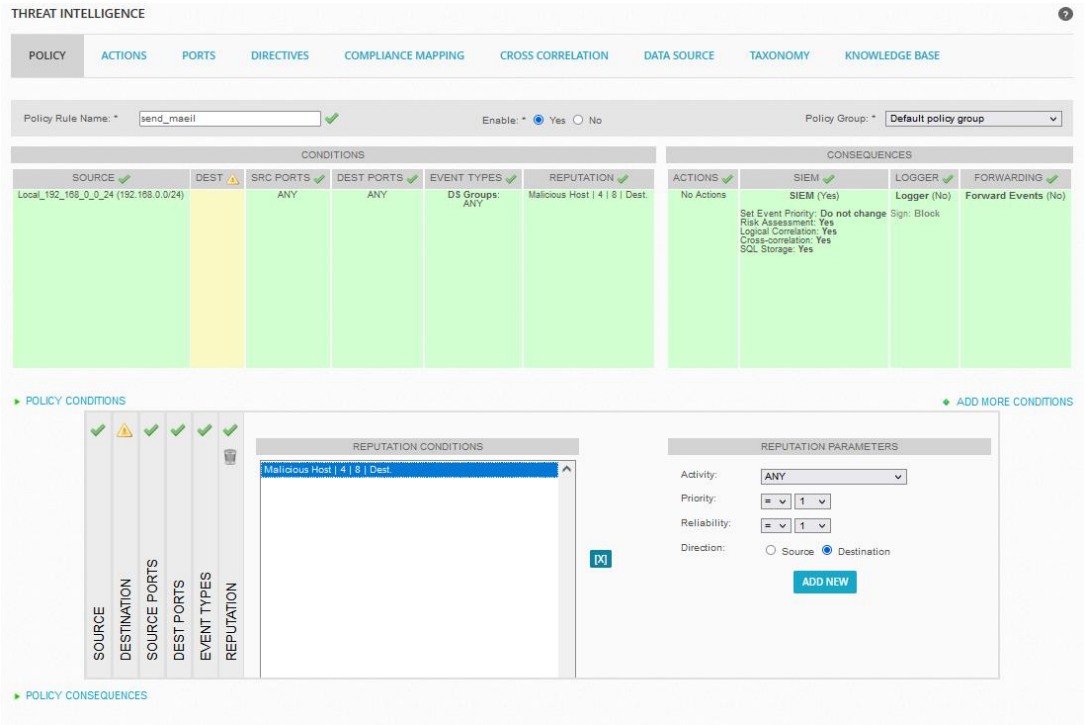


Рис 3.16. Налаштування Reputation Parameters в AlienVault OSSIM

Тепер обидві умови "Destination" і "Reputation" видно в верхній частині сторінки.

Далі потрібно пов'язати дію з відправленням електронної пошти в якості наслідку.

Для створення наслідку, що включає в себе дію:

- Перейдіть до Configuration (Конфігурація) > Threat Intelligence (Інтелект безпеки) > Policy (Політика).
- Виберіть потрібне правило політики та натисніть кнопку "Modify" (Змінити).

- Прокрутіть сторінку вниз і розгорніть розділ "Policy Consequences" (Наслідки політики).
- У розділі "Actions" (Дії) оберіть необхідну дію з розділу "Available Actions" (Доступні дії) справа.
- Додайте її, натиснувши знак плюса (+), або перетягуючи її в розділ "Active Actions" (Активні дії).

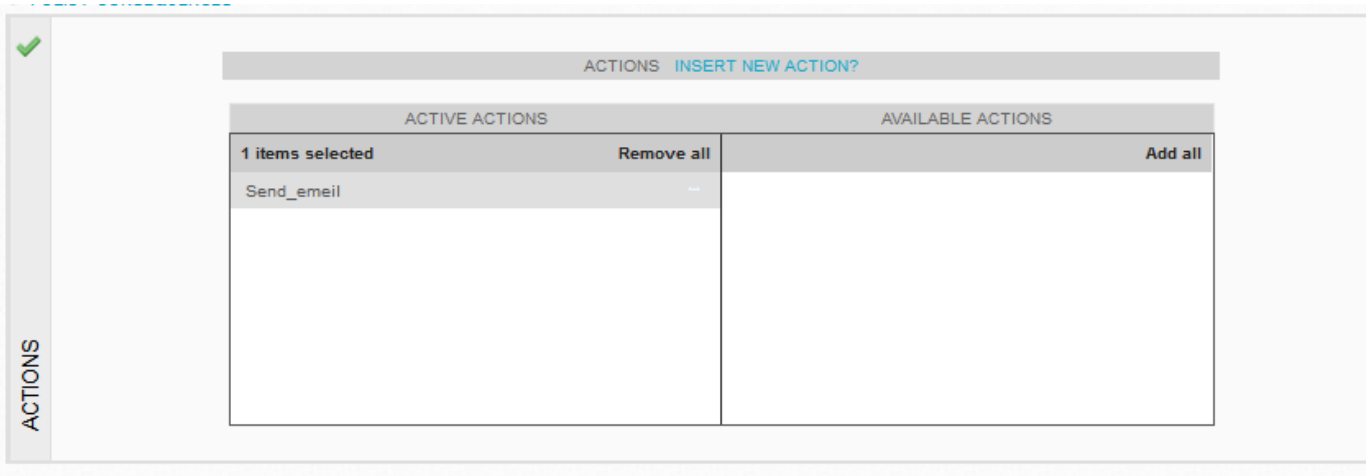


Рис 3.17. Включення створеної політики в AlienVault OSSIM

Натисніть кнопку Оновити політику, щоб зберегти зміни та вийти зі сторінки зміни політики.

Натисніть кнопку «Перезавантажити політики» на головній сторінці політик, щоб оновити та відобразити зміни.

3.3 Алгоритм сканування вразливостей кінцевих точок мережі за допомогою AlienVault OSSIM

AlienVault OSSIM - це комплексна система управління інформаційною безпекою, яка включає в себе вбудований сканер вразливостей. Сканер вразливостей

AlienVault OSSIM можна використовувати для сканування кінцевих точок, таких як комп'ютери, сервери та пристрої.

Для виконання сканування кінцевих точок за допомогою AlienVault OSSIM слід виконати наступні дії. Спочатку увійдіть в веб-інтерфейс AlienVault OSSIM та перейдіть до розділу «Environment». В цьому розділі оберіть опцію «Vulnerability». У вікні «Vulnerability» натискайте на кнопку «New Scan». Далі вкажіть назву сканування, виберіть сенсор (alienvault) та відповідний профіль сканування. Якщо необхідно, задайте розклад сканування (щодня, щотижня, щомісяця) та вкажіть IP-адреси або конкретну мережу для сканування.

Таблиця 3.1

Описи профілів сканування

Назва профілю	Опис
Base	Цей профіль сканування містить NVTs, які збирають інформацію про цільові системи. Він використовує Ping і Nmap для визначення того, чи працює хост, і збирає інформацію про операційну систему (OS). Він не виявляє вразливості.
Discovery	Цей профіль сканування містить NVTs, які надають інформацію про цільові системи. Він збирає інформацію про відкриті порти, використане апаратне забезпечення, брандмауери, встановлене програмне забезпечення та сертифікати, а також використовувані служби. Він не виявляє вразливості.
Full and fast	Цей профіль сканування містить NVTs, які не завдають шкоди цільовим системам. Спочатку він виконує сканування портів для отримання інформації про систему і використовує відповідні NVT на основі отриманої інформації для завершення сканування. Ці NVT

	оптимізовані для зниження вірогідності помилкових від'ємних результатів.
Full and fast ultimate	Цей профіль сканування розширює профіль Full and fast NVTs, які можуть вплинути на роботу служб чи систем, або навіть призвести до їх вимкнення. Спочатку він виконує сканування портів для отримання інформації про систему і використовує відповідні NVT на основі отриманої інформації для завершення сканування. Ці NVT оптимізовані для зниження вірогідності помилкових від'ємних результатів.
Full and very deep	Цей профіль сканування базується на профілі Full and fast, але не враховує результатів сканування портів. Іншими словами, він включає NVTs, які чекають на тайм-аут, і NVTs, які перевіряють вразливості програми, яка не була виявлена, роблячи сканування дуже повільним.
Full and very deep ultimate	Цей профіль сканування розширює профіль Full and very deep NVTs, які можуть вплинути на роботу служб чи систем, або навіть призвести до їх вимкнення. Сканування дуже повільне.
Aggressive	Цей профіль сканування виконує всі скрипти, пов'язані з вразливістю, незалежно від того, чи вони безпечні для сканованої цілі. Це може призвести до значного зниження продуктивності, а також виникнення проблем, таких як Відмова в обслуговуванні (DoS), несправності та помилки.
Host discovery	Цей профіль сканування містить NVTs, які використовують Ping для визначення того, чи працює хост. Він не виявляє вразливості.
System discovery	Цей профіль сканування містить NVTs, які використовують Ping для визначення того, чи працює хост, і Nmap для збору інформації про ОС та апаратне забезпечення. Він не виявляє вразливості.

Далі потрібно натиснути кнопку "Save". Після цього сканування автоматично стартує у визначений час і його стан можна перевірити в розділі «Vulnerability» - «Scan Jobs».

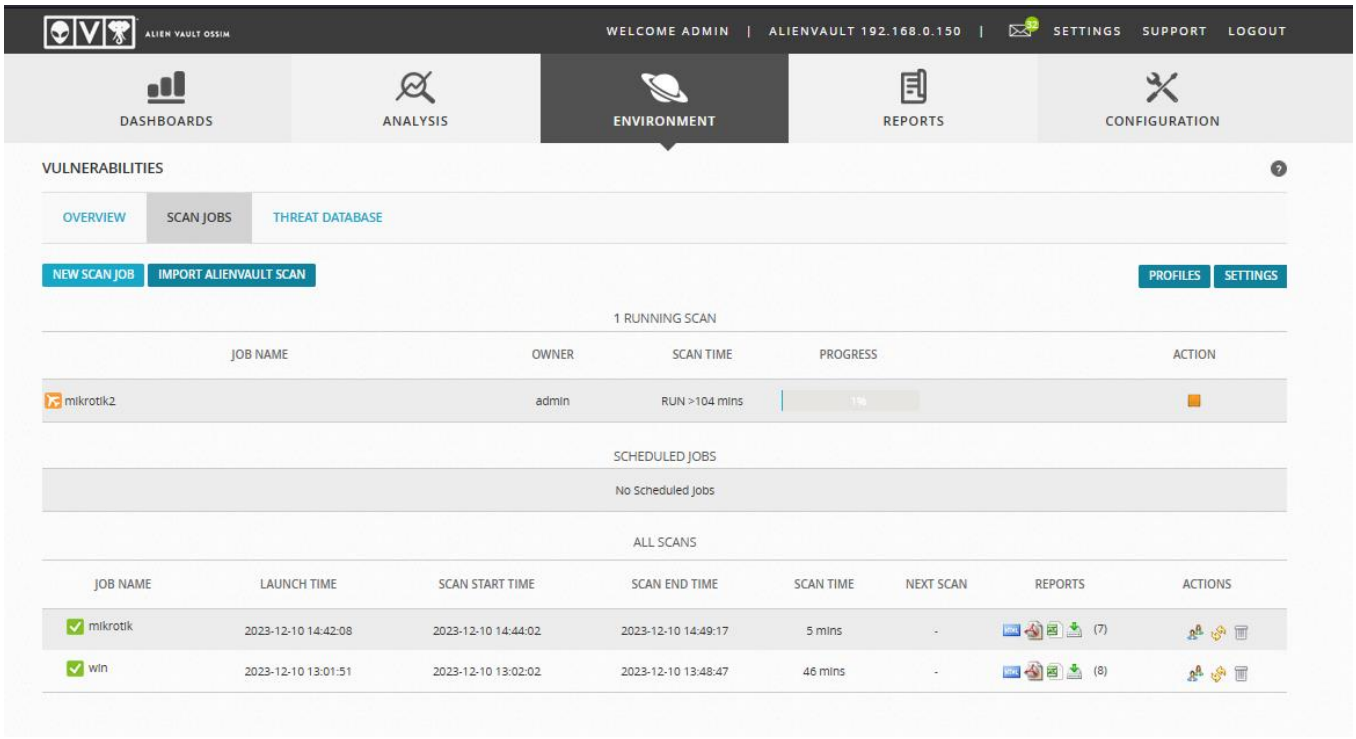


Рис 3.19. Інтерфейс Scan Jobs в AlienVault OSSIM

Сканер вразливостей AlienVault OSSIM почне сканувати вказані цілі на наявність відомих вразливостей. Після завершення сканування в результатах сканування буде відображено список виявлених вразливостей.

FTP Banner Detection	10092	ftp (21/tcp)	Info
References:**Vulnerability Detection Result:** **Remote FTP server banner:** **220 MikroTik FTP server (MikroTik 7.12.1) ready** **This is probably (a):** **- MikroTik RouterOS** **Server operating system information collected via "SYST" command:** **215 UNIX MikroTik 7.12.1** **CVSS Base Vector:** **AV:N/AC:L/Au:N/C:N/I:N/A:N** **Summary:** **This Plugin detects and reports a FTP Server Banner.** **CVSS Base Score:** **0.0**	Family name: Product detection Category: infos Created: 2005-11-03T13:08:04Z Modified: 2022-02-16T13:39:14Z		
Services	**10330**	**ftp (21/tcp)**	**Info**
References:**Vulnerability Detection Result:** **An FTP server is running on this port.** **Here is its banner :** **220 MikroTik FTP server (MikroTik 7.12.1) ready** **CVSS Base Vector:** **AV:N/AC:L/Au:N/C:N/I:N/A:N** **Summary:** **This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.** **CVSS Base Score:** **0.0**	Family name: Service detection Category: infos Created: 2011-01-14T09:12:23Z Modified: 2021-03-15T10:42:03Z		
Services	**10330**	**ssh (22/tcp)**	**Info**
References:**Vulnerability Detection Result:** **An ssh server is running on this port** **CVSS Base Vector:** **AV:N/AC:L/Au:N/C:N/I:N/A:N** **Summary:** **This routine attempts to guess which service is running on the remote ports. For instance, it searches for a web server which could listen on another port than 80 or 443 and makes this information available for other check routines.** **CVSS Base Score:**	Family name: Service detection Category: infos Created: 2011-01-14T09:12:23Z Modified: 2021-03-15T10:42:03Z		

Рис 3.20. Приклад знайдених вразливостей в AlienVault OSSIM

3.4 Рекомендації щодо технологій виявлення та реагування на кіберінциденти в інформаційній системі організації на базі AlienVault OSSIM

AlienVault OSSIM - це комплексне рішення для виявлення та реагування на кіберінциденти (SIEM). Воно дозволяє отримувати, обробляти та аналізувати дані з різних джерел, таких як мережеві пристрої, системи безпеки, веб-сервери тощо. Це дає можливість виявляти потенційні загрози та інциденти на ранніх стадіях.

Для ефективного виявлення та реагування на кіберінциденти на базі AlienVault OSSIM необхідно дотримуватися таких рекомендацій:

- Встановіть та налаштуйте AlienVault OSSIM відповідно до рекомендацій виробника. Це включає в себе настройку джерел даних, політик тригерів та інших параметрів.
- Регулярно оновлюйте AlienVault OSSIM. Це дозволить отримувати доступ до останніх даних та правил виявлення загроз.
- Інтегруйте AlienVault OSSIM з іншими системами безпеки. Це дозволить отримувати більш повну картину стану інформаційної системи організації.
- Розробіть та впровадьте політику виявлення та реагування на кіберінциденти. Це допоможе забезпечити ефективність виявлення та реагування на інциденти.

Рекомендації щодо виявлення кіберінцидентів

Для ефективного виявлення кіберінцидентів необхідно використовувати різні джерела даних. Це дозволить отримувати більш повну картину стану інформаційної системи організації та підвищити шанси на виявлення потенційних загроз та інцидентів на ранніх стадіях.

AlienVault OSSIM дозволяє отримувати дані з таких джерел:

- Мережеві пристрої: маршрутизатори, комутатори, брандмауери тощо.
- Системи безпеки: антивірусні продукти, системи виявлення вторгнень тощо.
- Веб-сервери: веб-сервери, веб-додатки тощо.
- Системи операційної безпеки: системи управління обліковими записами, системи управління доступом тощо.

Для виявлення кіберінцидентів можна використовувати такі методи:

- Аналіз журналів: аналіз даних, що зберігаються в журналах систем та пристроїв.
- Кореляція подій: виявлення зв'язків між подіями з різних джерел.
- Аналіз аномалій: виявлення відхилень від нормального стану інформаційної системи.

Рекомендації щодо реагування на кіберінциденти

Для ефективного реагування на кіберінциденти необхідно мати план реагування, який включає в себе такі етапи:

- Ідентифікація інциденту: визначення того, що сталося та чи є це інцидентом.
- Оцінка інциденту: оцінка масштабу та потенційних наслідків інциденту.
- Реагування на інцидент: вжиття заходів для усунення інциденту та мінімізації його наслідків.
- Розслідування інциденту: визначення причин інциденту та розробка заходів для запобігання його повторенню.

AlienVault OSSIM дозволяє автоматизувати деякі етапи реагування на кіберінциденти, такі як:

- Повідомлення про інцидент: надсилання повідомлень про інцидент відповідним особам.
- Ізоляція інциденту: ізоляція інциденту від інших систем та пристроїв.
- Відновлення системи**:** відновлення системи до стану до інциденту.

Додаткові рекомендації

Для підвищення ефективності виявлення та реагування на кіберінциденти на базі AlienVault OSSIM можна дотримуватися таких додаткових рекомендацій:

- Використовуйте правила виявлення загроз, які адаптовані до вашої інформаційної системи.
- Регулярно переглядайте правила виявлення загроз, щоб врахувати зміни в інформаційній системі та поточних загрозах.
- Залучайте до виявлення та реагування на кіберінциденти кваліфікованих фахівців.

Виконання цих рекомендацій допоможе вам підвищити ефективність виявлення та реагування на кіберінциденти в інформаційній системі організації.

ВИСНОВКИ

Досліджена проблема виявлення та реагування на кіберінциденти в інформаційній системі організації підкреслює актуальність та значущість цього аспекту для організацій. Кіберзагрози стають все більш вдосконаленими, вимагаючи відповідних та ефективних методів реагування для забезпечення безпеки інформації.

Проаналізовані різноманітні підходи до виявлення та реагування на кіберінциденти в інформаційних системах підкреслюють необхідність впровадження комплексного підходу. Врахування унікальних особливостей організаційної інфраструктури та вибір оптимального підходу є важливим етапом в процесі забезпечення ефективної кібербезпеки.

Аналіз існуючих методів та засобів виявлення та реагування на кіберінциденти в інформаційній системі організації визначає важливі тенденції розвитку області кібербезпеки. Використання передових технологій, таких як штучний інтелект, машинне навчання та аналіз великих даних, виявляється як обіцяні напрямки для ефективного виявлення та відповіді на кіберінциденти.

AlienVault OSSIM є потужним інструментом для забезпечення кібербезпеки, завдяки своїй відкритій архітектурі та універсальності. Система забезпечує ефективний моніторинг і реагування на події, інтегруючи різноманітні джерела даних. Її можливості сприяють створенню повного обзору кіберзагроз, що робить AlienVault OSSIM привабливим вибором для організацій, що прагнуть підвищити рівень своєї кібербезпеки.

Аналіз методів та засобів виявлення та реагування на кіберінциденти в інформаційній системі організації на базі AlienVault OSSIM свідчить про важливість інтегрованої платформи для моніторингу та аналізу подій безпеки. Застосування такої системи може значно полегшити процеси виявлення та відповіді на кіберзагрози, забезпечуючи комплексний погляд на безпеку інформаційної інфраструктури організації.

Отже, в ході цієї дослідницької роботи було проведено глибокий аналіз інтегрованої платформи AlienVault OSSIM як ефективного інструменту для виявлення та реагування на кіберінциденти в інформаційних системах організацій. Аналіз показав, що AlienVault OSSIM володіє значущими перевагами, такими як система виявлення вторгнень, інтеграція з відкритою платформою обміну інформацією про кіберзагрози (Open Threat Exchange) і відкритий вихідний код, що сприяє активному розвитку та адаптації до змін у кіберсередовищі. Результати роботи вказують на те, що AlienVault OSSIM може бути ефективним інструментом для забезпечення кібербезпеки, забезпечуючи комплексний моніторинг та аналіз подій безпеки. Враховуючи його переваги та відкритий характер, використання AlienVault OSSIM може допомогти організаціям підвищити рівень захисту своєї інформаційної інфраструктури та ефективно реагувати на сучасні кіберзагрози.

ПЕРЕЛІК ПОСИЛАНЬ

Як SIEM може захистити ваш бізнес від кіберзагроз URL https://dnif.medium.com/how-siem-can-safeguard-your-business-f9f30b7e6224 (дата звернення 06.12.2023).

Зубок М.І. Інформаційна безпека в підприємницькій діяльності / М.І. Зубок. – К.: ГНОЗІС, 2015 – 216с. (дата звернення: 06.12.2023).

9 кращих інструментів SIEM: Посібник з інформації про безпеку та управління подіями URL https://instagalleryapp.com/chistij-administrator-2/9-krashhih-instrumentiv-siem-posibnik-z-informacii/ (дата звернення: 09.12.2023).

OSSIM: a Careful, Free and Always Available Guardian for Your Network URL https://dl.acm.org/doi/fullHtml/10.5555/2642922.2642924 (дата звернення: 08.12.2023).

NIST Спеціальна публікація 1271 URL https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.ukr.pdf (дата звернення: 08.12.2023).

AlienVault: Threat Hunting/Network Analysis URL https://www.hackingarticles.in/alienvault-threat-hunting-network-analysis/ (дата звернення: 09.12.2023).

Tutorial: Create a Policy to Send Emails Triggered by Events URL https://cybersecurity.att.com/documentation/usm-appliance/policy-management/process-pol-send-emails.htm?tocpath=Documentation%7CUSM%20Appliance%E2%84%A2%7CUser%20Guide%7CPolicy%20Management%7C_____5 (дата звернення: 08.12.2023).

Configure Mail Relay in USM Appliance URL https://cybersecurity.att.com/documentation/usm-appliance/initial-setup/configuring-mail-relay.htm (дата звернення: 08.12.2023).

[Network Scan]How to scan Network Hosts and work with incident tickets Using AlienVault URL https://takahiro-oda.medium.com/network-scan-how-to-scan-network-

hosts-and-work-with-incident-tickets-using-alienvault-8fd1e2308dae (дата звернення: 08.12.2023).

Detect Advanced Threats withEndpoint Detection and Response (EDR) URL https://www.orion.pl/wp-content/uploads/2018/08/Detect-Advanced-Threats-with-Endpoint-Detection-and-Response-EDR.pdf (дата звернення: 06.12.2023).

What is SIEM? The Ultimate Guide to Security Information and Event Management URL https://www.logpoint.com/en/blog/what-is-siem/ (дата звернення: 07.12.2023).

OSSIM Update - Sysmon Logs Integrated OSSIM - Brute Force Alarm Triggered URL https://www.youtube.com/watch?v=pO_zG7VXIvY&ab_channel=RelativeSecurity (дата звернення: 07.12.2023).