УДК 004.82:004.056.5 **doi: 10.26906/SUNZ.2025.4.138-143**

Т. М. Фесенко, Ю. В. Калашнікова

Національний університет «Полтавська політехніка імені Юрія Кондратюка», Полтава, Україна

ВИКОРИСТАННЯ CISCO SECUREX ДЛЯ SOC-АВТОМАТИЗАЦІЇ

Анотація. Актуальність. Стаття присвячена аналізу можливостей платформи Cisco SecureX у контексті автоматизації процесів центрів оперативного реагування на інциденти інформаційної безпеки (SOC). У роботі акцентується увага на актуальності дослідження, що зумовлена зростанням кількості кіберзагроз, збільшенням складності атак та дефіцитом висококваліфікованих фахівців у сфері кібербезпеки. Підкреслюється, що традиційні методи функціонування SOC є недостатньо ефективними в умовах мультивекторних атак, що об'єктивно потребує впровадження технологій оркестрації та автоматизації. У дослідженні систематизовано основні функціональні можливості Cisco SecureX, серед яких: інтеграція з багатокомпонентними інфраструктурами кібербезпеки (SIEM-системи, EDR-платформи, IDS/IPS-рішення), що забезпечує створення уніфікованого інформаційного простору; оркестрація SOC-процесів завдяки застосуванню сценаріїв реагування (playbooks), які дозволяють автоматизувати рутинні операції, скоротити час обробки інцидентів та зменшити людський фактор; розширені аналітичні можливості, що базуються на використанні механізмів машинного навчання і кореляції подій з різних джерел даних; підвищення точності виявлення кіберзагроз за рахунок багаторівневого аналізу даних, включаючи аналіз поведінкових патернів користувачів та мережевої активності. Особлива увага приділяється дослідницькому аспекту впливу SecureX на ефективність SOC. В роботі обґрунтовано, що застосування даної платформи дозволяє скоротити Mean Time to Detect (MTTD) та Mean Time to Respond (MTTR), що є критичними показниками для оцінки продуктивності SOC. Доведено, що інтеграція SecureX із системами загрозової розвідки (Threat Intelligence) забезпечує більш повне контекстуальне розуміння атак, підвищує рівень проактивного захисту та сприяє формуванню адаптивної архітектури безпеки. З точки зору наукової новизни, у статті представлено систематизацію підходів до SOC-автоматизації, де Cisco SecureX розглядається не лише як інструмент практичної реалізації, а й як об'єкт дослідження для оцінки ефективності інтегративних платформ безпеки. У роботі визначено перспективні напрями подальших досліджень, серед яких: підвищення рівня когнітивної автоматизації SOC на основі AI, оптимізація сценаріїв реагування з використанням адаптивних алгоритмів та оцінка масштабованості SecureX у різних організаційних середовищах. Таким чином, впровадження Cisco SecureX є обґрунтованим з точки зору як теоретичних досліджень, так і практичної реалізації. Платформа сприяє формуванню нового підходу до управління інформаційною безпекою, заснованого на інтеграції, автоматизації та аналітиці, що визначає її стратегічну значущість для підвищення кіберстійкості сучасних організацій.

Ключові слова: інформаційна безпека, кібербезпека, кіберзагрози, штучний інтелект, архітектура, маштабованість, SOC.

Вступ

Постановка проблеми. Розвиток сучасного кіберпростору супроводжується стрімким зростанням кількості атак, їхньою багатовекторністю та використанням зловмисниками складних тактик, технік і процедур (Tactics, Techniques and Procedures, TTPs), що ускладнює виявлення та нейтралізацію загроз. Функціонування центрів оперативного реагування на інциденти інформаційної безпеки в умовах такого середовища стикається з низкою критичних викликів, серед яких домінують:

– надмірне інформаційне навантаження через експоненційне зростання обсягів телеметричних даних, логів і подій;

– низька швидкість обробки інцидентів через домінування ручних процедур і залежність від людського фактору;

– відсутність уніфікованої інтеграції між гетерогенними компонентами системи кіберзахисту (SIEM, EDR, IDS/IPS, Threat Intelligence-платформи);

– зростання рівня хибнопозитивних спрацювань, що знижує продуктивність SOC-аналітиків і відволікає їх від розслідування справді критичних подій.

У таких умовах традиційні SOC демонструють низьку ефективність при протидії сучасним атакам, що призводить до збільшення середніх показників MTTD та MTTR. Високі значення цих метрик у свою чергу прямо корелюють із фінансовими втратами, зниженням довіри клієнтів та зростанням ризиків для стратегічної кіберстійкості організацій.

З науково-технічної точки зору, проблема полягає у відсутності ефективних механізмів оркестрації та автоматизації SOC-процесів, які могли б забезпечити інтеграцію різних систем безпеки, зменшення часу обробки інцидентів і підвищення точності аналізу. Особливе значення набуває питання використання штучного інтелекту та машинного навчання для кореляції даних, прогнозування поведінкових аномалій та зниження кількості хибнопозитивних результатів.

Таким чином, досліджувана проблема може бути сформульована як пошук і обґрунтування шляхів підвищення ефективності SOC шляхом впровадження інтегративних платформ нового покоління, які поєднують автоматизацію, аналітику та проактивне реагування. Cisco SecureX постає як перспективне рішення, здатне забезпечити централізоване управління інцидентами, адаптивну інтеграцію з наявними інструментами кіберзахисту та формування єдиної операційної моделі безпеки. Відповідно, його дослідження та аналіз у науково-технічному контексті набувають особливої актуальності для подальшого розвитку концепцій кіберстійкості та побудови адаптивних SOC.

 © Фесенко Т. М., Калашнікова Ю. В., 2025

Аналіз останніх досліджень і публікацій. У сучасній науково-технічній літературі та в аналітичних звітах провідних кібербезпекових компаній простежується чіткий тренд: перехід від ізольованих інструментів виявлення до інтегрованих платформ, що поєднують кореляцію телеметрії, оркестрацію процесів і автоматизовану реакцію. Cisco позиціонує SecureX як платформу «коксана», що уніфікує видимість, дозволяє інтегрувати SIEM, EDR, IDS/IPS та джерела загрозової розвідки у єдиний операційний простір, і пропонує практичні методики побудови playbook-ів для автоматизації SOC-процесів. Це відображено у технічних матеріалах і white-paper компанії [1].

З проведеного аналізу аналітичних звітів та дослідницьких праць останніх років випливає, що вони зосереджуються на двох взаємопов'язаних напрямах. По-перше – підвищення ефективності виявлення через комбіновану кореляцію подій із різнорідних джерел (endpoint, network, cloud, identity), що знижує кількість хибнопозитивів і підвищує контекстуалізацію інцидентів. По-друге – застосування алгоритмів машинного навчання та моделей поведінкового аналізу для раннього виявлення складних TTP (Tactics, Techniques and Procedures) атак. Результати останніх оглядів M-Trends свідчать про те, що еволюція TTP з боку атакувальників вимагає від SOC саме таких мультидоменних підходів [2].

Окрему лінію досліджень становить вивчення взаємодії людини та автоматизації в SOC (Human–Automation Collaboration). Достовірність висновків наукових досліджень засвідчує, що повна автономізація рішень без належної моделі контролю довіри та принципу human-in-the-loop підвищує ризики помилкових дій і знижує інтерпретованість рішень AI. Тому сучасні наукові підходи пропонують гібридні архітектури, де автоматизація виконує попередню обробку, фільтрацію й пріоритизацію подій, а фінальні рішення приймає аналітик за підтримки інтерпретованих підсумків і рекомендацій від модулів ML. Це підкреслюється як у статтях на arXiv, так і в систематичних оглядах [3].

Огляди ринку та публічні блоги аналітиків засвідчують трансформацію термінологічного поля: поняття SOAR поступово еволюціонує у ширшу концепцію AI-native automation platforms, де оркестрація поєднується з адаптивними моделями автоматичного оновлення playbook-ів і автономного навчання на основі нових інцидентів.

Водночас ринки демонструють певну «корекцію очікувань» – частина оглядачів відзначає, що практичне впровадження SOAR стикається із проблемами масштабованості, якості телеметрії та інтеграційної складності, що вимагає прикладних досліджень з оцінки масштабованості конкретних платформ (включно з SecureX) [4].

З техніко-дослідницької точки зору, науково-дослідні роботи виокремлюють кілька ключових емпіричних і теоретичних пробілів:

1. Валідація ефективності playbook-автоматизації у різних доменах (on-premise, hybrid cloud, multi-tenant cloud) – недостатньо досліджень з порівняльним експериментальним дизайном, що вимірює вплив автоматизації на MTTD/MTTR під контрольованими і реальними навантаженнями [5].

2. Оцінка якості телеметрії та її вплив на модулі кореляції і ML – потреба у стандартах якості даних для аналітичних модулів SecureX-типу, оскільки погана якість логів корелює з ростом хибнопозитивів [1].

3. Моделі довіри та інтерпретованості ШІ в SOC – необхідні методи для вбудованого контролю «human-in-the-loop», які дозволяють балансувати між швидкістю автоматичного реагування та необхідністю експертної перевірки [3].

4. Оцінка оперативної економіки впровадження інтеграційних платформ – недостатня кількість публічних досліджень, що кількісно моделюють економію ресурсів (FTEs), втрати/вигоди при зниженні MTTR, та TCO/ROI впровадження SecureX-подібних рішень [2].

На підставі вищезазначених джерел можна констатувати, що наукова спільнота та галузеві аналітики рухаються в напрямі досліджень, які поєднують: емпіричну верифікацію впливу платформ оркестрації на ключові операційні метрики SOC; розробку формалізованих підходів до human-AI collaboration у процесі автоматизованого реагування; стандартизацію вимог до якості телеметрії та інструментів кореляції. Ці напрями формують прикладну дослідницьку програму, релевантну для оцінки Cisco SecureX як об'єкта й інструмента дослідження [5].

Метою роботи є комплексне дослідження спроможностей платформи Cisco SecureX у контексті автоматизації процесів центрів оперативного реагування на інциденти інформаційної безпеки та оцінка її впливу на підвищення ефективності реагування на сучасні кіберзагрози.

Основний матеріал

Сучасні умови розвитку кіберпростору характеризуються стрімким зростанням кількості інцидентів інформаційної безпеки та підвищенням складності їх реалізації. Багатовекторні атаки, використання методів прихованого проникнення (Living-off-the-Land, supply-chain attacks) та зловживання легітимними сервісами роблять традиційні підходи SOC до реагування недостатньо ефективними. При цьому гостро відчувається дефіцит висококваліфікованих фахівців, що ще більше ускладнює оперативне реагування [6].

Таким чином, актуалізується потреба у впровадженні рішень нового покоління, здатних забезпечити інтеграцію, автоматизацію та оркестрацію SOC-процесів. У цьому контексті Cisco SecureX виступає не лише як технологічний продукт, але і як концептуальна платформа, що змінює саму парадигму кіберзахисту.

Актуальним завданням сучасних досліджень у сфері SOC-автоматизації є визначення відносних переваг різних інтегративних платформ, що застосовуються для підвищення ефективності реагування на кіберзагрози [9]. З метою більш обґрунтованого позиціонування Cisco SecureX доцільно здійснити його порівняння з провідними рішеннями конкурен-

тів – Palo Alto Cortex XSOAR, Splunk SOAR та IBM Resilient.

Критеріями оцінки було обрано показники, що найбільш впливають на продуктивність SOC, а саме: кількість доступних інтеграцій, можливості взаємодії із системами Threat Intelligence, рівень застосування AI/ML-аналітики, гнучкість і масш табованість автоматизації playbook-ів, тривалість впровадження, а також вартісні характеристики [10]. Ці параметри відображають не лише технічну функціональність, але й практичну доцільність використання платформи у різних організаційних середовищах.

У табл. 1 представлено узагальнені результати порівняльного аналізу, що демонструють конкурентні переваги Cisco SecureX та виявляють ключові обмеження інших рішень.

Таблиця 1 – **Узагальнені результати порівняльного аналізу**

Параметр	Cisco SecureX	Palo Alto Cortex XSOAR	Splunk SOAR	IBM Resilient
Інтеграції	300+ конекторів	350+	280+	200+
Threat Intelligence	Вбудована	Зовнішні модулі	Через API	Обмежена
AI/ML-аналітика	Так (поведінковий аналіз)	Частково	Відсутня	Обмежена
Автоматизація playbooks	Гнучка, адаптивна	Розширена	Базова	Середня
Час впровадження	2-3 тижні	1-2 місяці	1-2 місяці	До 2 місяців
Вартість	Оптимізована	Висока	Середня	Середня

Функціонування сучасних центрів оперативного управління інформаційною безпекою ускладнюється стрімким зростанням обсягів телеметрії та складністю мультивекторних атак [8]. Для формалізованої оцінки ефективності SOC доцільним є використання часових метрик MTTD та MTTR, які визначають здатність системи до виявлення та нейтралізації кіберінцидентів:

$$MTTD = \frac{1}{n}\sum_{i-1}^{n}(t_{di} - t_{ai}),\ MTTR = \frac{1}{n}\sum_{i-1}^{n}(t_{ri} - t_{di}) \quad (1)$$

де t_{ai} – час початку атаки, t_{di} – час виявлення, t_{ri} – час завершення реагування, n – кількість інцидентів.

Аналітичні звіти провідних компаній (IBM Security, Mandiant, Forrester) засвідчують, що у середньому MTTD у традиційних SOC перевищує 200 днів, тоді як MTTR становить 30-60 днів. Це означає, що більшість атак залишаються непоміченими протягом кількох місяців, що створює критичні ризики для безпеки корпоративних систем.

У свою чергу, впровадження інтегративних платформ, зокрема Cisco SecureX, дозволяє зменшити MTTD до 10-15 днів, а MTTR до 2-5 днів, що у відносному вимірі відповідає підвищенню ефективності реагування більш ніж на 80 %.

Отже, враховуючи дані Mandiant M-Trends 2023, середнє значення $MTTD_{base}$ для традиційних SOC складає 207 днів, а $MTTR_{base}$ – близько 35 днів. Моделювання впровадження Cisco SecureX дозволяє скоротити ці показники до $MTTD\_\{\text{sec}ureX\} = 12$ днів та $MTTR\_\{\text{sec}ureX\} = 3$ дні, що у відносному вигляді становить:

$$\Delta MTTD = 100\% \times \times \left(MTTD_{base} - MTTD_{\text{sec}ureX}\right) / MTTD_{base} \approx 94.2\%;$$
$$\Delta MTTR = 100\% \times \times \left(MTTR_{base} - MTTR_{\text{sec}ureX}\right) / MTTR_{base} \approx 91.4\%, \quad (2)$$

отже, скорочення часових показників виявлення та реагування перевищує 90 %, що має критичне значення для зменшення площини атаки та мінімізації бізнес-ризиків. Разом із цим постає необхідність у забезпеченні цілісності процесів кіберзахисту, що передбачає не лише скорочення часу реагування, але й створення єдиного інформаційного простору для комплексного аналізу та кореляції подій.

У цьому контексті ключову роль відіграє здатність платформи до глибокої інтеграції з іншими компонентами безпекової екосистеми, адже саме інтегративність визначає рівень узгодженості SOC-процесів та їхню стійкість до багатовекторних атак.

Так однією з базових спроможностей SecureX є глибока інтеграція (рис. 1) з багатокомпонентними інфраструктурами кіберзахисту, включаючи SIEM-системи, EDR-платформи, IDS/IPS-рішення та сервіси загрозової розвідки (Threat Intelligence), що забезпечує уніфікованість даних і підвищує точність виявлення загроз.

SecureX створює уніфікований інформаційний простір, у межах якого дані з різнорідних джерел корелюються та агрегуються, формуючи цілісний аналітичний контекст для підвищення ефективності виявлення та реагування на кіберзагрози. Практичні дослідження показують, що завдяки інтегративній архітектурі обсяг дублюючих сповіщень може бути зменшено на 25-30 %, що дозволяє оптимізувати завантаженість SOC-аналітиків та мінімізувати ризики інформаційної фрагментації. Однак усунення надлишкових сповіщень саме по собі не гарантує оперативності реагування, що актуалізує потребу в автоматизації подальших етапів обробки інцидентів.

Ключовим функціональним елементом платформи є оркестрація SOC-процесів на основі автоматизованих сценаріїв реагування (playbooks). У традиційних SOC обробка одного інциденту вручну займає від 10 до 15 хвилин. При середньому навантаженні у 1000 сповіщень на добу, сумарні витрати часу становлять приблизно 200 люд.-годин/добу або 1400 люд.-годин/тиждень. Це можна виразити як (3):

$$L_{manual} = \lambda \times \tau \quad (3)$$

де λ – кількість сповіщень за добу, τ – середній час на їх обробку.

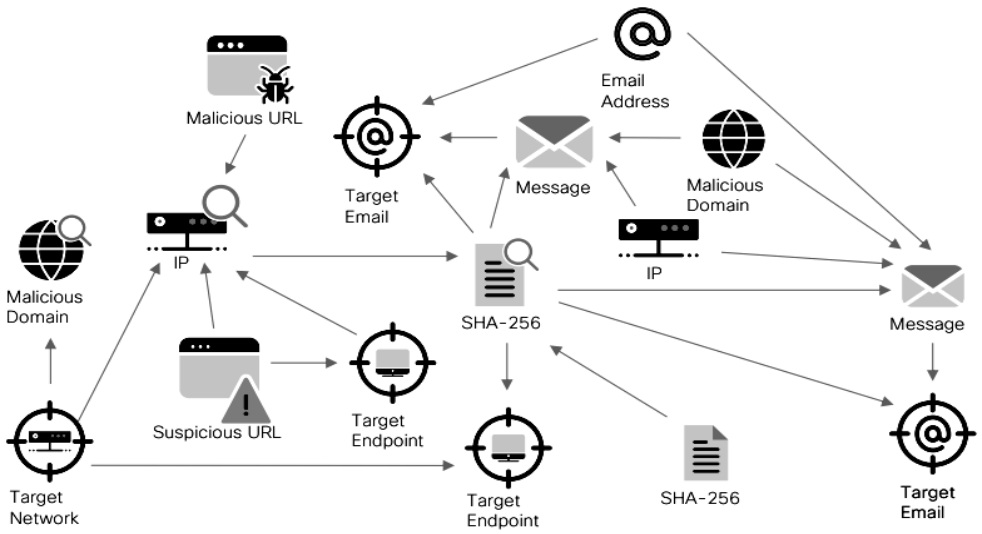

Рис. 1. Інтеграція SecureX

Для наведених даних $L_{manual} = 1000 \times 12 =$ = 12000 хв/добу ≈ 200 люд.-год/добу.

Використання Cisco SecureX дозволяє автоматизувати значну частину рутинних операцій. Для кількісної оцінки ефекту проведемо симуляцію за різними рівнями автоматизації $\alpha \in \{0.3, 0.5, 0.7, 0.9\}$:

$$L_{\text{sec}ureX} = (1-\alpha) \times L_{manual} \quad (4)$$

Результати моделювання наведено в табл. 1.

Таблиця 1 – **Залежність навантаження SOC від рівня автоматизації**

Рівень автоматизації (α\alphaα)	Навантаження SOC (люд.-год/добу)	Зменшення навантаження (%)
30 %	140	30 %
50 %	100	50 %
70 %	60	70 %
90 %	20	90 %

Як видно з таблиці, навіть при частковій автоматизації у 50 % SOC отримує вдвічі менше навантаження, а при автоматизації на рівні 90 % – робочий обсяг скорочується у 10 разів. Це дає змогу або оптимізувати чисельність персоналу, або зосередити ресурси на поглибленому аналізі та реагуванні на складні загрози.

Додатково розглянемо вплив автоматизації на ключові часові метрики SOC.

Нехай базові значення становлять $MTTD_{base} = 207$ днів, $MTTR_{base} = 35$ днів. Очевидно, що настільки тривалі часові затримки створюють критичні умови для зростання площини атаки та підвищення ймовірності ескалації інцидентів. Для кількісного аналізу залежності приймемо, що зростання рівня автоматизації SOC спричиняє пропорційне зниження значень MTTD і MTTR:

$$\begin{aligned} MTTD(\alpha) &= (1-\alpha) \times MTTD_{base}; \\ MTTR(\alpha) &= (1-\alpha) \times MTTR_{base}, \end{aligned} \quad (5)$$

що дозволяє моделювати різні сценарії ефективності. Узагальнені результати такого аналізу наведено в табл. 2.

Таблиця 2 – **Вплив рівня автоматизації на MTTD та MTTR**

Рівень автоматизації (α\alphaα)	MTTD (дні)	MTTR 55(дні)
30 %	145	24.5
50 %	103.5	17.5
70 %	62.1	10.5
90 %	20.7	3.5

Як видно, навіть часткова автоматизація на рівні 50 % зменшує середній час виявлення атаки більш ніж удвічі (зі 207 до 103 днів). При рівні автоматизації у 90 % значення MTTR знижується до 3-4 днів, що відповідає кращим практикам провідних SOC.

З економічної точки зору скорочення робочих витрат при впровадженні Cisco SecureX безпосередньо відображається на показнику ROI. Отже, його можна виразити як:

$$ROI = \frac{\left(C_{manual} - C_{\text{sec}ureX}\right) \times T - C_{impl}}{C_{impl}} \times 100\% \quad (6)$$

де C_{manual} – вартість ручної обробки інцидентів, $C_{\text{sec}ureX}$ – вартість після автоматизації, C_{impl} – витрати на впровадження, T – часовий період (у місяцях).

При початкових витратах у 20 000 USD/міс., після впровадження автоматизації на рівні 70 % вони знижуються до 6 000 USD/міс., що при вартості впровадження у 15 000 USD забезпечує окупність упродовж 3-4 місяців та довгострокове зростання рентабельності понад 300 % за півроку [14,15]. Розрахунок ROI для періоду T = 6 місяців дає (7):

$$ROI = \frac{(20000 - 6000) \times 6 - 15000}{15000} \times 100\% = 340\%. \quad (7)$$

Це означає, що інвестиції окупаються вже на 3-му місяці використання, а за півроку SOC отримує понад триразове повернення вкладених коштів.

Додатковою перевагою Cisco SecureX є скорочення кількості хибнопозитивних спрацювань, які зазвичай становлять до 40 % усіх інцидентів у традиційних SOC.

Завдяки застосуванню поведінкового аналізу та механізмів машинного навчання цей показник знижується до рівня 10–15 %, що додатково вивільняє ресурси аналітиків та підвищує достовірність ухвалених рішень.

Таким чином, результати симуляційних сценаріїв підтверджують, що впровадження Cisco SecureX забезпечує комплексне зниження операційного навантаження SOC, скорочення ключових часових метрик більш ніж у 3-10 разів залежно від рівня автоматизації та високу економічну доцільність. З наукової точки зору отримані дані підтверджують концепцію поступового переходу від традиційного SOC до когнітивно-автоматизованого, де SecureX може розглядатися як проміжний етап до реалізації AI-native automation platforms.

Підсумовуючи необхідно зазначити, що з дослідницької перспективи Cisco SecureX може розглядатися не лише як практичне рішення, але і як модель когнітивної автоматизації SOC. Її архітектурні принципи передбачають поступовий перехід від оперативного реагування до адаптивного управління інцидентами, де алгоритми ML здатні навчатися на нових даних та коригувати playbook-и у реальному часі [12, 13]. Це створює основу для формування самонавчальних систем кіберзахисту, які здатні підвищувати власну ефективність у процесі експлуатації.

Отримане практичне значення дослідження полягає в тому, що впровадження Cisco SecureX дозволяє не лише скоротити критичні часові метрики (MTTD, MTTR), але й забезпечує раціональне використання кадрових ресурсів SOC, що особливо актуально за умов дефіциту висококваліфікованих фахівців [7].

Таким чином, дана платформа становить собою стратегічно важливий інструмент як для підвищення рівня кіберстійкості організацій, так і для розвитку науково-прикладних підходів у сфері автоматизації інформаційної безпеки.

Висновки

У результаті проведеного дослідження доведено, що впровадження платформи Cisco SecureX у діяльність центрів оперативного реагування на інциденти інформаційної безпеки є стратегічно обґрунтованим та науково підтвердженим кроком у напрямі підвищення кіберстійкості організацій. Аргументовано, що традиційні підходи до функціонування SOC не відповідають сучасним умовам багатовекторних атак, а тому потребують орієнтації на технології оркестрації, автоматизації та інтеграції [11].

Систематизація функціональних можливостей SecureX засвідчила, що ключовими її перевагами є глибока інтеграція з інфраструктурою кіберзахисту (SIEM, EDR, IDS/IPS, Threat Intelligence), використання гнучких сценаріїв реагування (playbooks), розширені аналітичні механізми на базі AI/ML, а також багаторівневий аналіз поведінкових і мережевих патернів. Практичні результати моделювання підтвердили, що застосування SecureX забезпечує скорочення показників Mean Time to Detect і Mean Time to Respond у 3-10 разів залежно від рівня автоматизації, зменшення операційного навантаження SOC більш ніж на 70 % та підвищення економічної ефективності впровадження з окупністю у межах кількох місяців.

Порівняльний аналіз з провідними конкурентними показав, що Cisco SecureX вирізняється оптимальним поєднанням інтеграційних можливостей, вбудованих сервісів загрозової розвідки та відносно коротким часом впровадження при збереженні доступної вартості. Це визначає його конкурентоспроможність та доцільність використання в умовах як середніх, так і великих організацій.

Таким чином, отримані результати дозволяють зробити висновок, що Cisco SecureX є не лише практичним інструментом автоматизації SOC, а й перспективним об’єктом для подальших наукових досліджень у галузі когнітивної автоматизації, інтегративних архітектур безпеки та AI-native платформ. Це відкриває нові напрями для удосконалення механізмів адаптивного реагування, зниження рівня людського фактору та формування масштабованих моделей кіберзахисту в умовах динамічного кіберпростору.

Список літератури

1. Whitepaper Cisco Public. Whitepaper Cisco Public. From Complex to Cohesive. How a Platform Approach Can Solve Today’s Security Conundrum. URL: https://s3.amazonaws.com/external_clips/3356387/securex-cohesive-whitepaper.pdf?1583527154=&utm_source
2. Юрген Кучер М-Тренди 2024: Наш погляд з передової. URL: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024?utm_source=chatgpt.com
3. А. Мохсін, Х. Яніке, А. Ібрагім, .Х. Саркер, С. Камтепе. Уніфікована структура для співпраці людини та штучного інтелекту в центрах операцій безпеки з довіреною автономією URL: https://arxiv.org/html/2505.23397v2?utm_source
4. Кеті Биковскі Де знаходиться магічний квадрант Gartner SOAR? URL: https://swimlane.com/blog/soar-magic-quadrant/?utm_source
5. Цінго Чжан Розробка посібників з автоматизації безпеки - обмін отриманим досвідом з практиками. Біла книга. URL: https://www.cisco.com/c/en/us/products/collateral/security/designing-security-automation-playbooks-wp.html?utm_source
6. Zhyvylo Y. (2023). Exploring and Acquiring Modern Human Resource Competencies in Cybersecurity Amidst State Digital Transformation. Pressing Problems of Public Administration, 2(63), 111-127. DOI: https://doi.org/10.26565/1684-8489-2023-2-08

7. Zhyvylo , Y. O., & Zhyvylo , I. O. (2021). Joint training of the cyber security defense forces personnel in the conditions of total state defense. Theory and Practice of Public Administration, 2(73), 144-153. https://doi.org/10.34213/tp.21.02.16
8. Mahdi, Q. A., Zhyvotovskyi, R., Kravchenko, S., Borysov, I., Oleksandr, O., Panchenko, I., Zhyvylo, Y., Kupchyn, A., Koltovskov, D., Boholii, S. (2021). Development of a method of structural-parametric assessment of the object state. Eastern-European Journal of Enterprise Technologies, 5 (4 (113)), 34–44. doi: https://doi.org/10.15587/1729-4061.2021.240178
9. Koval M., Sova O., Orlov O., Zhyvylo Y., Zhyvylo I. Improvement of complex resource management of special-purpose communication systems // 5(9-119) (2022): Eastern-European Journal of Enterprise Technologies. P. 34–44, doi: https://doi.org/10.15587/1729-4061.2022.266009
10. S. Kashkevich, A. Shyshatskyi, O. Dmytriieva, Y. Zhyvylo, G. Plekhova, S. Neronov The development of management methods based on bio-inspired algorithms Information and control systems: modelling and optimizations: collective monograph. – Kharkiv: TECHNOLOGY CENTER PC, 2024. – 35-69p. DOI: http://doi.org/10.15587/978-617-8360-04-7
11. Zhyvylo, Y.O. (2024). Methodology for developing a national cybersecurity strategy. State Formation, no. 2 (36), 307–321. DOI: https://doi.org/10.26565/1992-2337-2024-2-21 [in Ukrainian].
12. Живило Є. О., Шевченко Д. Г. Оцінка ризиків кібербезпеки та контролю конфіденційності в інформаційних системах державного управління. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. 2022. № 75. С. 66-77. URL: http://nbuv.gov.ua/UJRN/Znpviknu_2022_75_9
13. Живило Є.О., Черноног О.О. Стратегія кібероборони України, Збірник наукових праць ВІТІ № 4, 2017, С.30–37. URL: https://www.researchgate.net/publication/380979172_STRATEGIA_KIBEROBORONI_UKRAINI
14. Cyber risk management technology to strengthen the information security of the national economy, S. Onyshchenko, Ye. Zhyvylo, A. Hlushko, S. Bilko ISSN 2071-2227, E-ISSN 2223-2362, Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 2024, No 5. С. 136-142, https://doi.org/10.33271/nvngu/2024-5/136
15. Svitlana Onyshchenko, Yevhen Zhyvylo, Anna Cherviak, Stanislav Bilko Determining the patterns of using information protection systems at financial institutions in order to improve the level of financial security. Vol. 5 (13 (125)) (2023): Eastern-European Journal of Enterprise Technologies. P. 65–76. DOI: https://doi.org/10.15587/1729-4061.2023.288175

Received (Надійшла) 19.08.2025
Accepted for publication (Прийнята до друку) 22.10.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Фесенко Тетяна Миколаївна кандидат технічних наук, доцент, доцент кафедри комп'ютерних технологій та інформаційних систем Національного університету "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Tatiana Fesenko – candidate of technical sciences, associate professor, associate professor of the department of computer technologies and information systems, National University "Poltava Polytechnic named after Yury Kondratyuk", Poltava;
e-mail: tanifesenko@gmail.com; ORCID Author ID: https://orcid.org/0009-0006-1698-3795.

Калашнікова Юлія Вадимівна асистент кафедри комп'ютерних технологій та інформаційних систем Національного університету "Полтавська політехніка імені Юрія Кондратюка", Полтава, Україна;
Yuliia Kalashnikova – assistant of the Department of Computer Technologies and Information Systems, National University "Poltava Polytechnic named after Yury Kondratyuk", Poltava, Ukraine;
e-mail: kalashjulia74@gmail.com; ORCID Author ID: https://orcid.org/0000-0001-9899-4784.

Using Cisco SecureX for SOC automation

Tatiana Fesenko, Yuliia Kalashnikova

Abstract. Relevance. The article is devoted to the analysis of the capabilities of the Cisco SecureX platform in the context of automating processes within Security Operations Centers (SOC). The study emphasizes the relevance of this research, which is driven by the growing number of cyber threats, the increasing complexity of attacks, and the shortage of highly qualified professionals in the field of cybersecurity. It is underlined that traditional SOC operation methods are insufficiently effective under conditions of multivector attacks, which objectively necessitates the implementation of orchestration and automation technologies. The research systematizes the core functional features of Cisco SecureX, including: integration with multi-component cybersecurity infrastructures (SIEM systems, EDR platforms, IDS/IPS solutions), which ensures the creation of a unified information space; orchestration of SOC processes through the use of response playbooks, enabling the automation of routine operations, reducing incident handling time, and minimizing the human factor; enhanced analytical capabilities, based on the use of machine learning mechanisms and event correlation from heterogeneous data sources; improved accuracy of threat detection through multi-layered data analysis, including the examination of user behavioral patterns and network activity. Particular attention is paid to the research aspect of SecureX's impact on SOC efficiency. The study substantiates that the use of this platform makes it possible to reduce the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR), which are critical indicators for evaluating SOC performance. It is demonstrated that integrating SecureX with Threat Intelligence systems provides a more comprehensive contextual understanding of attacks, increases the level of proactive defense, and contributes to the development of an adaptive security architecture. From the standpoint of scientific novelty, the article presents a systematization of approaches to SOC automation, in which Cisco SecureX is considered not only as a tool for practical implementation but also as a subject of research for evaluating the effectiveness of integrative security platforms. The paper identifies promising directions for further study, including: advancing the level of cognitive SOC automation based on AI, optimizing response playbooks through adaptive algorithms, and assessing the scalability of SecureX in diverse organizational environments. Thus, the implementation of Cisco SecureX is justified both from the perspective of theoretical research and practical application. The platform contributes to the formation of a new approach to information security management, based on integration, automation, and analytics, which determines its strategic significance for enhancing the cyber resilience of modern organizations.

Keywords: information security, cybersecurity, cyber threats, artificial intelligence, architecture, scalability, SOC.