SCIENTIFIC COLLECTION INTERCONF

№ 44
March, 2021

THE ISSUE CONTAINS:

Proceedings of the 8th International Scientific and Practical Conference

SCIENTIFIC RESEARCH IN XXI CENTURY

OTTAWA, CANADA

6-8.03.2021

InterConf
Scientific Publishing Center

SCIENTIFIC COLLECTION «INTERCONF»

№ 44 | March, 2021

THE ISSUE CONTAINS:

Proceedings of the 8th International Scientific and Practical Conference

SCIENTIFIC RESEARCH IN XXI CENTURY

OTTAWA, CANADA

6-8.03.2021

OTTAWA
2021

UDC 001.1

S 40 *Scientific Collection «InterConf»*, (44): with the Proceedings of the 8th International Scientific and Practical Conference «Scientific Research in XXI Century» (March 6-8, 2021). Ottawa, Canada: Methuen Publishing House, 2021. 784 p.

ISBN 978-0-458-20903-3

EDITOR COORDINATOR

EDITORIAL BOARD

If you have any questions or concerns, please contact a coordinator Mariia Granko.

The recommended styles of citation:

1. Surname N. (2021). Title of article or abstract. *Scientific Collection «InterConf»,* (44): with the Proceedings of the 8th International Scientific and Practical Conference «Scientific Research in XXI Century» (March 6-8, 2021) in Ottawa, Canada; pp. 21-27. Available at: https://interconf.top/...
2. Surname N. (2021). Title of article or abstract. *InterConf,* (44), 21-27. Retrieved from https://interconf.top/...

This issue of Scientific Collection «InterConf» contains the International Scientific and Practical Conference. The conference provides an interdisciplinary forum for researchers, practitioners and scholars to present and discuss the most recent innovations and developments in modern science. The aim of conference is to enable academics, researchers, practitioners and college students to publish their research findings, ideas, developments, and innovations.

TABLE OF CONTENTS

PART I

LIGHT INDUSTRY AND FOOD INDUSTRY

GENERAL ENGINEERING AND MECHANICS

MODELING AND NANOTECHNOLOGY

INFORMATION AND WEB TECHNOLOGIES

MILITARY AFFAIRS AND NATIONAL SECURITY

Сєвєрінов Олександр Васильович

ORCID ID: 0000-0002-6327-6405

кандидат технічних наук, доцент кафедри безпеки інформаційних технологій

Харківський національний університет радіоелектроніки, Україна

Коломійцев Олексій Володимирович

ORCID ID: 0000-0001-8228-8404

Заслужений винахідник України, доктор технічних наук,

старший науковий співробітник, професор кафедри

Національного технічного університету

"Харківський політехнічний університет", Україна

Альошин Геннадій Васильович

ORCID ID: 0000-0003-1876-7616

доктор технічних наук, професор кафедри

Українська державна академія залізничного транспорту, Україна

Голубничий Дмитро Юрійович

ORCID ID: 0000-0002-6873-7004

кандидат технічних наук, доцент, доцент кафедри Інформаційних систем Харківський

національний економічний університет імені Семена Кузнеця, Україна

Третяк Вячеслав Федорович

ORCID ID: 0000-0003-2599-8834

кандидат технічних наук, доцент, науковий співробітник наукового центру

Повітряних Сил Харківський національний університет

Повітряних Сил імені Івана Кожедуба, Україна

Власов Андрій Володимирович

ORCID ID: 0000-0001-6080-237

кандидат технічних наук, старший науковий співробітник

наукового центру Повітряних Сил

Харківський національний університет Повітряних Сил

імені Івана Кожедуба, Україна

Лисиця Аліна Олександрівна

ORCID ID: 0000-0002-2156-7765

аспірантка, інженер 1 категорії кафедри Національний технічний університет

"Харківський політехнічний університет, Україна

АНАЛІЗ СИСТЕМ АНАЛІТИКИ ПОВЕДІНКИ КОРИСТУВАЧІВ ТА СУТНОСТЕЙ

Процес інформатизації суспільства призводить до того, що інформаційний ресурс стає одним з головних джерел економічної ефективності будь-якого підприємства або організації. Тому в сучасному суспільстві всі сфери життєдіяльності підприємства стають залежними від інформаційного розвитку, а його конкурентоспроможність в значній мірі залежить від уміння захищати свою ділову, комерційну, технічну і фінансову інформацію, персональні дані фізичних осіб. Кожне сучасне конкурентоспроможне підприємство має конфіденційну інформацію, при цьому в більшості випадків придбання цієї інформації вимагало значних витрат.

У зв'язку з цим в даний час все більше посилюється небезпека втручання в роботу інформаційних систем підприємства в формі несанкціонованого доступу до інформації. Сьогодні існують досить потужні системи несанкціонованого збору інформації, високоефективні технічні засоби і досить якісно підготовлені фахівці. Діяльність, пов'язана з несанкціонованим збором інформації про промислові та комерційні таємниці, називається промисловим шпигунством [1-5]. Наслідками успішного несанкціонованого доступу можуть стати компрометація або спотворення конфіденційної інформації, нав'язування неправдивої інформації, порушення встановленого порядку збирання, обробки та передачі інформації, відмови і збої в роботі технічних систем.

Безпека інформаційних ресурсів та інформаційних технологій є одним з найбільш важливих факторів успішної діяльності комерційних або державних підприємств.

При забезпеченні інформаційної безпеки організації одним з видів діяльності є виявлення інцидентів інформаційної безпеки. Неможливо уникнути всіх інцидентів інформаційної безпеки, так як завжди можуть відбуватися події, що тягнуть за собою потенційну загрозу.

Інцидент інформаційної безпеки - одне або серія небажаних або несподіваних подій в системі інформаційної безпеки, які мають імовірність скомпрометувати ділові операції і поставити під загрозу захист інформації [1-5].

Як випливає з статистики з розвитком інформаційних систем загрози, які виходять від власних співробітників організацій, стали дуже серйозними, а збиток від їх дій обчислюється десятками мільярдів доларів.

Відомо достатньо методів боротьби з інцидентами. Одним з найбільш ефективних методів з урахуванням необхідності контролю своїх співробітників є впровадження систем аналітики поведінки користувачів та сутностей – User and Entity Behavior Analytics (UEBA)). UEBA-системи збирають дані про системні оточення - хости, додатки, мережевий трафік і системи зберігання даних. Це дозволяє проводити аналіз взаємодії операторів і обладнання, забезпечуючи повну видимість робочих процесів, і ідентифікувати більш широкий клас загроз, пов'язаних не тільки з користувачами, але і з об'єктами IT-інфраструктури [1-5].

У зв'язку з цим актуальним є вивчення питань управління інцидентами інформаційної безпеки на основі використання UEBA систем.

На даний час системи UEBA являються як окремими рішеннями, так і функціями, що вбудовані в інші платформи безпеки.

Використання UEBA-систем дозволяє перейти до пошуку аномалій не тільки в поведінці користувачів, але і сутностей, до яких відносять робочі станції, мережне обладнання, програмне забезпечення, мережний трафік та інше. Ці рішення дозволяють захиститися від самих різних загроз, таких як несанкціонований доступ та виток конфіденційної інформації, шахрайські дії, крадіжки прав доступу, дії вірусів та шкідливого ПЗ і багато інших.

UEBA-системи надають розгорнуту інформацію по інцидентах, включаючи інформацію про всіх задіяних користувачах і системах, з аналізом певних аномалій в їх поведінці, що значно спрощує подальше розслідування.

Принцип роботи систем UEBA заснований на зборі даних про дії користувачів і сутностей з системних журналів та інших джерел в корпоративній мережі організації (систем DLP, SIEM, хмарних сховищ, баз даних та інших). Системи застосовують передові аналітичні методи для аналізу даних і встановлюють базові моделі поведінки користувачів (патерн). UEBA постійно відстежує поведінку об'єкта і порівнює його з базовою поведінкою (патерном) для того ж об'єкта або схожих об'єктів, щоб виявити ненормальну поведінку. Крім цього, UEBA-системи можуть будувати моделі поведінки цілих груп користувачів і визначати відхилення кожного з них від загальної моделі.

Якщо якісь дії користувача вибиваються з побудованої моделі, UEBA-система визначає це як аномальну активність і створює відповідне попередження адміністратору безпеки. Зазвичай це відбувається в режимі реального часу або близькому до нього.

Рішення UBA виявляють аномалії з використанням аналітичних методів, що включають машинне навчання, статистичні моделі, правила і сигнатури погроз.

Системи UEBA ведуть ретроспективну статистику по кожному користувачу і на основі зібраних даних по його аномальної активності здатні виставляти своєрідні оцінки ризику кожному з них. Надалі ці оцінки використовуються в ранжируванні подій, полегшуючи роботу адміністратора безпеки.

В системах UEBA встановлюється базова оцінка – межа, після якої система визначає поведінку як потенційну загрозу. Система UEBA порівнює встановлену базову оцінку з поточною поведінкою користувача, обчислює оцінку ризику і визначає, чи припустимі відхилення. Якщо оцінка ризику перевищує певний поріг, система сповіщає аналітиків безпеки в режимі реального часу (рис. 1).

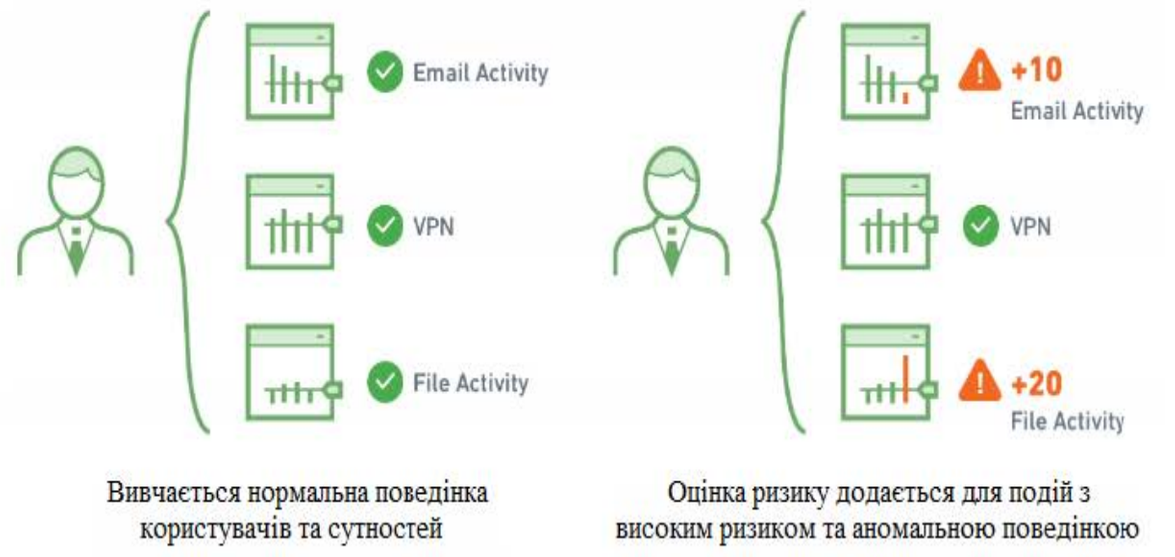

Рис. 1. **Додавання оцінки ризиків при аналізі поведінки**

Системи UEBA виявляють будь яку аномальну поведінка або випадки, коли є відхилення від «нормальних» патернів. Система працює наступним чином:збирає інформацію про типову поведінку користувача в конкретному середовищі (наприклад, виявляє список програм, сайтів, які людина використовує зазвичай на робочому місці); вибудовує модель типової поведінки; при аналізі виявляє аномальну активність і в разі її виникнення моментально реєструє і розцінює як потенційну загрозу.

Вибудовування моделі типової поведінки користувача здійснюється за допомогою як простих методів статистичного аналізу, так і машинного навчання. У разі компрометації даних дії зловмисника будуть різко відрізнятися від дій власника облікового запису.

Наприклад, системі UEBA потрібно побудувати модель використання працівником X VPN-серверів. Система починає фіксувати атрибути підключень, включаючи час початку і кінця сесії, країну підключення, IP-адреси та інше кожен раз, коли X буде заходити в мережу. Потім по кожному з атрибутів вибудовується модель і проаналізувати її, система виявляє, що є нормою, а що - відхиленням. Якщо система будує модель по країнам підключення VPN-серверів, що використовує X, то після кожного заходу X в мережу, UEBA регіструє данні про країну підключення (рис. 2).

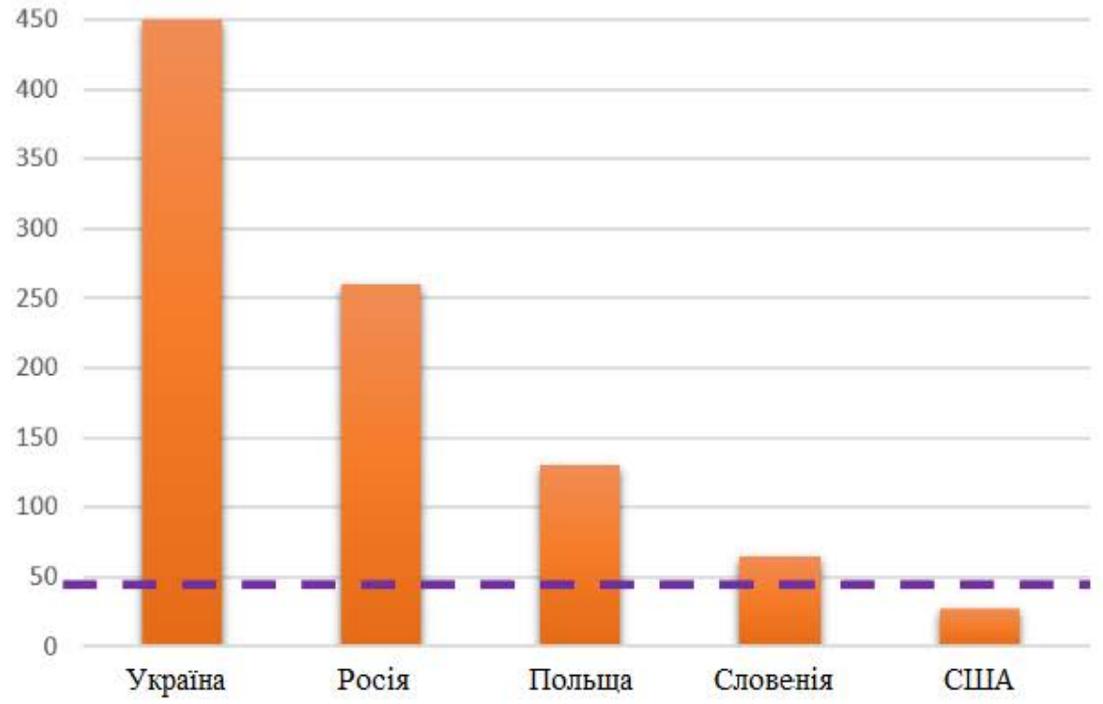

Рис. 2. **Частота використання VPN-серверів X по країнам**

Як тільки буде встановлена межа нормальної активності, UEBA зможе легко ідентифікувати аномальні дії. На діаграмі рисунку 2 фіолетова лінія відображає поведінковий поріг (базову оцінку) X. VPN з України, Росії, Польщі та Словенії будуть вважатися нормою. Будь-які VPN-з'єднання з країнами, частота підключень до яких буде нижче, ніж зі Словенією, будуть потрапляти в зону ризику.

В ядро будь якої UEBA-системи включаються технології по роботі з великими масивами даних. І якщо у випадку з розширеннями до відомих SIEM-систем (IBM QRadar UBA, HPE ArcSight UBA, LogRhythm AI Engine) такі технології доступні від виробника, то самостійні рішення повинні або використовувати сторонні розробки (наприклад, Exabeam використовує Elastic Stack), або свої власні (Splunk UBA, Microsoft ATA).

Також UEBA-система здатна вирішити такі завдання як зловживання правами привілейованих облікових записів і виявлення підозрілого часу підключення. Більшість співробітників компаній працюють по конкретному графіку і приходять в один і той же час, йдучи точно в строк. Коли

співробітник є інсайдером і планує скопіювати важливу інформацію зі свого комп'ютера для передачі третім особам, він може залишитися на роботі допізна або прийти раніше початку робочого дня, для того щоб інші співробітники не змогли звернути увагу на те, чим він займається. Системи поведінкового аналізу зможуть відстежити аномальну активність і передати дані співробітникові, відповідальному за безпеку.

Системи UEBA також можуть збирати дані, які співробітники мають в своїх звітах і журналах, а також аналізувати інформацію про файлах, потоки і пакети.

UEBA-системи надають розгорнуту інформацію по інцидентах, включаючи інформацію про всіх задіяних користувачах і системах, з аналізом певних аномалій в їх поведінці, що значно спрощує подальше розслідування.

Системи класу UEBA - важливий елемент у виявленні невідомих типів загроз, APT-атак, а також співробітників, що порушують правила ІБ всередині компанії.

Продукти UEBA націлені на вирішення чотирьох базових задач.

1. Проста і розширена аналітика інформації з різних джерел із застосуванням методів машинного навчання, періодично або постійно, в режимі реального часу.

2. Призначені для оперативного детектування атак і інших аномалій, які зазвичай не виявляються класичними засобами ІБ.

3. Визначення значимості подій, зібраних з різних джерел (системи типу SIEM, DLP, AD і т.п.) З метою швидкого реагування адміністраторами з інформаційної безпеки.

4. Потужна реакція на події, забезпечена за рахунок того, що адміністратори по ІБ володіють комплексною і детальної інформації про інцидент.

Результати порівняльного аналізу основних з розглянутих UEBA-систем як по загальним характеристикам, так і функціоналу з виявлення інцидентів представлені в таблиці 1 .

Таблиця 1

Порівняння сучасних UEBA-систем

UEBA-система / Параметр	Exabeam Advanced Analytics	Splunk UBA	Microsoft Advanced Threat Analytics	MicroFocus ArcSight UBA	IBM QRadar UBA	Forcepoint UEBA	Securonix UEBA
Відкритий вихідний код		Так					Так
Хмарні середовища	Немає даних	Так	Так	Немає даних	Немає даних	Немає даних	Так
Локальне програмне забезпечення	Так	Так	Так	Так	Так	Так	Так
Просунута аналітика	Так		Так		Так		Так
Реагування на інциденти		Так	Так	Так	Так		Так
Машинне навчання	Так	Так	Так		Так	Так	Так
Видимість дій користувачів через звіти і інфопанелі	Так	Так	Так	Так		Так	Так
Сповіщення в реальному часі	Так	Так	Так	Так			Так
Інструментарій криміналістичної експертизи	Так	Так	Так			Так	Так
Повідомлення, що налаштовуються		Так					
Рольової доступ до звітів	Так				Так		
Звіти про погрози		Так		Так	Так	Так	
Модель ліцензування, заснована на сутностях	Немає даних	Так	Так	Тільки HP UEBA	Немає даних	Немає даних	Немає даних
Інтеграція з технологіями	IAM, DLP	SIEM	SIEM, IAM	SIEM	SIEM	SIEM, DLP	SIEM, IAM, DLP
Збір логів з SaaS-додатків		Так					Так

Продовження таблиці 1

Логі та призначений для користувача контекст даних з Active Directory	Так	Так	Так		Так	Так	Так
Логі подій безпеки з кінцевої точки	Так	Так	Так				Так
Мережний потік / Пакетні дані	Так	Так	Так				Так
Неструктуровані контекстні дані		Так					Так
Збір логів з ОС, додатків, сервісів	Так	Так	Так				Так
Метадані електронних повідомлень		Так				Так	Так
Статистичні моделі	Так	Так	Так				Так
Моделювання на основі правил і підписів	Так		Так		Так		Так
Піймання базовою моделлю користувачів з аномальним поведінкою на старті				Так	Так		Так
Адаптація системи до динамічних змін користувачів	Так	Так		Так	Так	Так	Так

Проведений аналіз підтвердив той факт, системи класу UEBA - важливий елемент у виявленні невідомих типів загроз, APT- атак, а також співробітників, що порушують правила ІБ всередині компанії. Крім того, виробники програмних продуктів UEBA світового рівня представляють на ринок системи корпоративного класу зі зручним інтерфейсом, широкими можливостями контролю та аналітичними функціями.

Принцип роботи систем UEBA заснований на зборі даних про дії користувачів і сутностей з системних журналів та інших джерел в корпоративній мережі організації (систем DLP, SIEM, хмарних сховищ, баз

даних). Системи застосовують передові аналітичні методи для аналізу даних і встановлюють базові моделі поведінки користувачів (патерн). Рішення UBA виявляють аномалії з використанням аналітичних методів, що включають машинне навчання, статистичні моделі, правила і сигнатури погроз.

Крім того, незважаючи на широкий функціонал та можливості систем UEBA, вони не можуть працювати окремо. Тому на даний час спостерігається тенденція до створення комплексних систем управління інцидентами та інформаційною безпекою, які поєднують системи UEBA з системами управління інформаційною безпекою та подіями безпеки (SIEM), системами управління ідентифікацією і доступом (IAM), системами запобіганню витоку конфіденційних даних (DLP).

Список джерел:

1. Информационная безопасность: учеб, пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. В. Лаптев. - Краснодар:КубГАУ, 2020. - 332 с.
2. Информационная политика и безопасность: учебное пособие / авторсоставитель Безродный В.П. - Донецк: ДонНУ, 2020. - 175 с.
3. Третяк, В., & Пашнєва, А. (2017) Оптимізація структури сховища даних у вузлах інфокомунікаційної мережі хмарного середовища. Системи управління, навігації та зв'язку. № . 4 (44). – С. 122-128.
4. Коломійцев, О., Голубничий, Д., Коц, Г., Третяк, В., Євстрат, Д., & Лисиця, А. (2020). Задачі дискретної оптимізації та їх постановка для розміщення засобів захисту в розподіленій системі. Збірник наукових праць ΛΟΓΟΣ, 36-41. https://doi.org/10.36074/20.11.2020.v5.12
5. Третяк, В., Голубничий, Д., Коломійцев, О., Мегельбей, Г., Возний, О., & Філіпенков, О. (2020). Математична модель рангового підходу. Збірник наукових праць ΛΟΓΟΣ, 116-122. https://doi.org/10.36074/25.12.2020.v1.40

SCIENTIFIC EDITION

BN 978-0-458209-03
9 780458 209033

SCIENTIFIC COLLECTION «INTERCONF»

№ 44 | March, 2021

The issue contains:

Proceedings of the 8th International
Scientific and Practical Conference

**SCIENTIFIC RESEARCH
IN XXI CENTURY**

OTTAWA, CANADA
6-8.03.2021

Published online: March 15, 2021
Printed: March 30, 2021. Circulation: 200 copies.

Contacts of the editorial office:

Scientific Publishing Center «InterConf»
E-mail: info@ interconf.top
URL: https://www.interconf.top

InterConf
Scientific Publishing Center