УДК 65.012.8

Бєгун А.В., к.е.н., професор,
Осипова О.І., к. е. н., доц.,
Урденко О.Г., аспірант,
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

Biehun, A.V., Dr. Prof.,
Osipova O.I., Associate Professor,
Urdenko, O.G., postgraduate ,
SHEE «Kyiv National Economic University
named after Vadim Hetman»

СИТУАЦІЙНИЙ ЛОГ-МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

SITUATIONAL LOG-MANAGEMENT OF INFORMATION SECURITY OF THE ENTERPRISE

Анотація. Сучасні тенденції в розвитку IT-систем призводять до підвищення рівня складності IT-инфраструктури. Однією із основних причин збільшення такої складності є необхідність забезпечення інформаційної безпеки кожного домену. В першу чергу це пов'язано із стрімким розповсюдженням хмарних сервісів і мобільних пристроїв співробітниками та клієнтами компаній.

У статті проведено дослідження питання ситуаційного лог-менеджменту подій інформаційної безпеки. Для забезпечення комплексного рішення безпеки та моніторингу подій інформаційної безпеки авторами запропоновано скористатися програмною платформою для моніторингу логів, яка базується на технології хмарних обчислень. Зокрема, розглянуто основні напрями вирішення завдань щодо забезпечення комплексного рішення безпеки, а саме впровадження систем класу SIEM (наприклад, IBM Security QRadar SIEM, HP ArcSight, Tibco Loglogic, McAfee NitroSecurity, Symantec SSIM, RSA Envision, Splunk, LogRhythm) та використання сервісів для лог-менеджменту й аналітики, що базуються на хмарних обчисленнях (наприклад, Stackify або Loggly). Визначено, що використання SIEM-системи потребує значних обчислювальних ресурсів на підприємстві, тому в цьому контексті сервіси, які базуються на технології хмарних обчислень, мають ряд переваг. Тому для моніторингу подій інформаційної безпеки авторами запропоновано скористатись сервісом Loggly, що базується на технології хмарних обчислень.

Авторами досліджено основні інструменти сервісу Loggly та на конкретному прикладі проілюстровано, що ці інструменти дозволяють зручно організувати збір логів системи та додатків від різних джерел, нормалізувати лог-дані та провести їх аналіз. Розглянуто тарифи та умови використання хмарного сервісу Loggly залежно від особливостей та індивідуальних вимог компанії. На основі проведеного дослідження виділено основні переваги використання сервісу Loggly для збору та аналізу даних лог-журналів.

Ключові слова: лог, лог-менеджмент, хмарні обчислення, критичні події, джерело загрози, інциденти інформаційної безпеки, криптографічний протокол.

Annotation. Modern trends in the development of IT systems lead to an increase in the complexity of IT infrastructure. One of the main reasons for increasing such complexity is the need to provide information security for each domain. First of all, this is due to the rapid spread of cloud services and mobile devices by employees and clients of companies.
The article deals with the issue of situational log management of information security events. To provide an integrated security solution and monitor information security events, the authors propose using a software platform for monitoring logs based on cloud computing technology. In particular, the main directions of solving the tasks to provide a comprehensive security solution, namely, the introduction of SIEM class systems (for example, IBM Security QRadar SIEM, HP ArcSight, Tibco Loglogic, McAfee NitroSecurity, Symantec SSIM, RSA Envision, Splunk, LogRhythm) and the use of services for logging management and cloud-based analysts (e.g. Stackify or Loggly). It has been determined that the use of SIEM systems requires significant computing resources at the enterprise, so in this context services based on cloud computing technology have a number of advantages. Therefore, for the purpose of monitoring information security events, the authors suggested using Loggly, a technology based on cloud computing.
The authors examine the main tools of the Loggly service and, on a concrete example, illustrate that these tools allow you to conveniently organize the collection of logs of the system and applications from different sources, normalize log data and analyze them. The tariffs and terms of use of loggly service cloud service are considered depending on the features and individual requirements of the company. Based on the research, the main advantages of using Loggly service for collecting and analyzing log log data are highlighted.
Keywords: log, log management, cloud computing, critical events, source of threat, information security incidents, cryptographic protocol.

Вступ. Новітні тенденції та технології розвитку IT-систем створюють умови підвищення рівня складності IT-інфраструктури. Однією з головних причин збільшення такої складності є забезпечення інформаційної безпеки (ІБ) кожного домену. Якщо раніше для захисту, наприклад, локальної мережі достатньо було придбати більш дорогий брандмауер і встановити його в єдиній точці входу/виходу даних, то зараз використання хмарних сервісів, а також мобільних пристроїв співробітників і клієнтів компаній створює проблему дослідження й розробки «платформи» — інструментів комплексного рішення безпеки. Одним із таких інструментів є сервіс для лог-менеджменту та аналітики, який базується на технології хмарних обчислень [4].

У кожному домені ІБ на основі політики інформаційної безпеки домену здійснюється моніторинг усіх процесів [2] і рівня інформаційної безпеки.

Відповідно до терміну «платформа» визначимо основні задачі, які необхідно вирішувати в кожному домені ІБ:

1) збір даних — логів від різних джерел інформації (журнали подій серверів і робочих станцій, мережеве активне обладнання, DLP-системи, IDS та IPS-системи, антивірусні програми);

2) нормалізація логів від різних джерел — процес переведення записів лог-журналів у єдиний стандартний вид;

3) фільтрація та кореляція подій безпеки;

4) стосовно політики безпеки домену, реєстрація деяких подій як інцидентів ІБ.

Здійснивши огляд ринку готових ІТ-рішень, пропонуються можливі напрями вирішення поставлених завдань:

1) впровадження систем класу SIEM (IBM Security QRadar SIEM, HP ArcSight, Tibco Loglogic, McAfee NitroSecurity, Symantec SSIM, RSA Envision, Splunk, LogRhythm);

2) використання сервісів для лог-менеджменту та аналітики, що базуються на хмарних обчисленнях. Наприклад, Stackify або Loggly.

Використання SIEM-системи потребує значних обчислювальних ресурсів. У цьому контексті сервіси, які базуються на технології хмарних обчислень, мають ряд переваг [3].

За даної технології розподіленої обробки даних комп'ютерні ресурси й потужності надаються користувачеві як Інтернет-сервіси [1]. За рахунок цього забезпечується:

- зниження рівня вимог до обчислювальної потужності персональних комп'ютерів компанії;
- економія дискового простору (дані зберігаються на віддалених серверах провайдера);
- відсутність витрат на покупку програмного забезпечення (ПЗ) — усі потрібні програми беруться в оренду у провайдера хмарних обчислень;
- висока відмовостійкість;
- висока швидкість обробки даних;
- незалежність від елементів управління інформаційною інфраструктурою.

Викладення основного матеріалу. Враховуючи зазначені переваги, для вирішення поставлених завдань і моніторингу подій інформаційної безпеки, пропонується скористатися програмною платформою для моніторингу логів, яка базується на технології хмарних обчислень, на прикладі сервісу Loggly.

Loggly — це SaaS solution («Програмне забезпечення як послуга») — сервіс для лог-менеджменту та аналітики, який базується на технології хмарних обчислень (компанія заснована у 2009 році у Сан-Франциско, штат Каліфорнія).

Даний сервіс допомагає системним аналітикам, командам технічної підтримки обробляти та аналізувати значні масиви даних журналів логів, які надходять із різноманітних джерел — додатків, платформ та операційних систем.

Найпоширенішимиі джерелми, з яких можна збирати дані лог-файлів для аналізу, є:

1. Операційні системи: Linux, Windows.

2. Серверні додатки:

2.1. Local file or Syslog: файл-моніторинг (Linux Files, Windows Files), стандартні додатки (Apache, Nginx, Tomcat, IIS, MS SQLServer, MySQL, Rails, Django, MongoDB), Development Libraries (Java Log4j, PHP, PHP Monolog), Deployment Automation (Puppet, Chef, Docker), Log Collectors (FluentD, Logstash).

2.2. Пряма відправка із додатків: Development Libraries (Java Logback, Node.js, Django, Python, Ruby), Endpoints (Syslog, HTTP/S Event Endpoint, HTTP/S Bulk Endpoint).

2.3. Хмарні платформи: AWS Cloudtrail, Heroku, S3, New Relic, Webhooks.

3. Клієнтські додатки:

3.1. Web-клієнти: Javascript, Tracking Pixel, Flash, HTTP/S Event Endpoint, HTTP/S Bulk Endpoint.

3.2. Development Libraries: Python, Ruby, iOS, Java Logback, .NET.

4. Мережеві пристрої та Роутери.

Шляхи відправлення даних до сервісу представлені в табл. 1.

Таблиця 1

СПОСОБИ ВІДПРАВЛЕННЯ ДАНИХ ДО СЕРВІСУ LOGGLY

№	Спосіб	Опис
1	Local Syslog Agent	Використання локального системного агента (наприклад, syslog Windows) для відправки даних у Loggly
2	Centralized Syslog Agent	Централізація усіх лог-даних перед відправкою до Loggly шляхом використання
3	Hardware Device	Відправка даних з апаратних пристроїв (роутерів, файєрволів), використовуючи протоколи UDP, TCP
4	Direct With No Agent	Прямий спосіб, без використання агентів. Можливим є налаштування додатків таким чином, щоб запис логів здійснювався безпосередньо до Loggly через протокол HTTP / S, використовуючи RESTful API
5	Client-Side Logging	Безпосередньо з браузера або пристрою кінцевого користувача, використовуючи RESTful API або Tracking pixels

*Розроблено авторами

Система дозволяє записувати у форматі реального часу та обробляти будь-які текстові формати логів (наприклад, json, sys-

log) від syslog-ng, rsyslog, nxlog, Snare, routers, switches, Ruby, Java, Python, C/C++, Javascript, PHP, Apache server, Tomcat, MySQ.

Під час проведення дослідження використовувався хмарний сервіс Loggly для аналізу лог-даних журналів системи, визначення подій ІБ та задання правил оповіщення про інциденти інформаційної безпеки. Результати проведеного дослідження наведено нижче.

Так, після реєстрації власного акаунту було здійснено імпорт даних, а саме даних операційної системи Windows: Журналу подій Windows, файлів журналів і потокового системного журналу.

Відправлені дані можна переглянути у двох форматах: syslog (текстовий формат даних, який дозволяє використовувати точну позначку часу створення повідомлення й здійснювати надійну ідентифікацію джерела повідомлення, а також застосовувати кодування UTF-8 для тексту повідомлення) та json (текстовий формат обміну даними, заснований на JavaScript і зазвичай використовуваний саме з цією мовою).

Трьома основними інструментами сервісу є:

1) Dashboard — інструмент, за допомогою якого можна відстежувати активність системи та додатків. Це, свого роду, «web-дошка», на якій за допомогою графіків і таблиць відображаються параметри працездатності системи та додатків. Кожен акаунт має Summary Dashboard — головну «дошку», на якій відображається (рис. 1):

- All Events Graph — графік, який відображає кількість усіх подій, які відправляються до Loggly;
- Alerts Overview — відображає критичні події системи;
- Saved Search Overview — перелік збережених пошуків акаунту;
- Top Values — відображає активність системи за значеннями обраного користувачем полів, яке найчастіше зустрічаються.

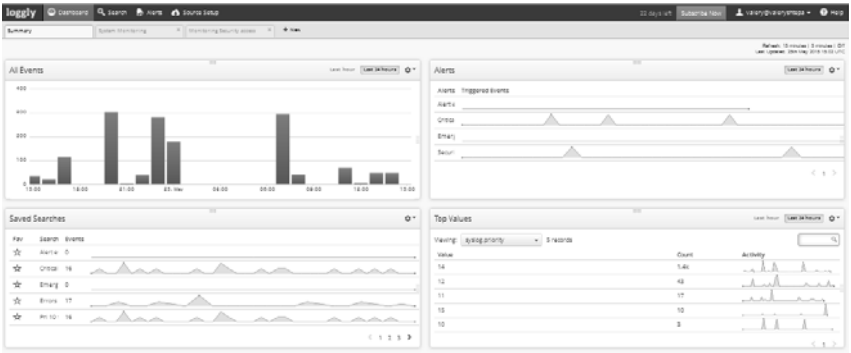

Рис. 1. Головна «дошка» Summary Dashboard акаунту

Крім того, є можливість створювати користувацькі дошки — «Custom Dashboard», залежно від потреби користувача (наприклад, для відображення метрик стабільності системи, подій додатків розробників тощо). До них можуть входити стандартні графіки сервісу та збережені пошуки користувача. Для Custom Dashboard діє розмежування прав доступу для різних користувачів акаунту.

2) Search — дозволяє здійснювати пошук (повнотекстовий пошук, пошук за окремими полями, значеннями змінних) за лог-файлам системи та додатків. Для зручності пошуку можливим є використання фільтрів.

Проведемо пошук за текстовим запитом «Security» за записами системних журналів за останні сім днів. Використаємо фільтр за параметрами: значення поля Severity (Важливість події) — «ERROR». На рис. 2 відображено результати пошуку за текстовим запитом «Security» за записами системних журналів періоду 17–24 травня із залученням фільтрації поля json.Severity: ERROR. Отримано такі результати пошуку: 41 подія, в полях лог-файлів яких присутнє слово «Security».

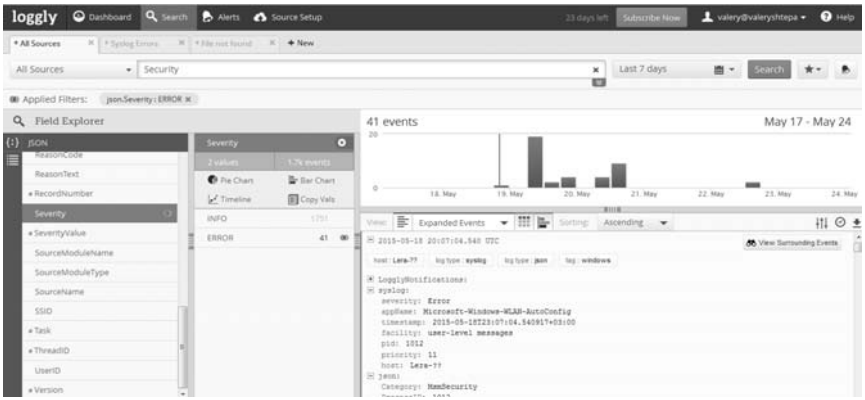

Рис. 2. Результати пошуку за текстовим запитом «Security»

Вміст лог-файлу кожної знайденої події можна прочитати, використовуючи інструмент View.

Дані логів подано у двох форматах syslog та json. Обираючи справа поле лог-файлу, можна переглянути усі можливі значення у знайдених результатах. Для зручності аналізу результати пошуку можна відображати графічно — у вигляді графіків, кругових і стовпчикових діаграм.

Побудований графік або діаграму можна додати до користувацької Custom Dashboard. Приклад створеної користувацької Custom Dashboard наведено на рис. 3.

Рис. 3. Користувацька Custom Dashboard «System Monitoring»

3) Alerts — інструмент, який дозволяє налаштувати оповіщення про критичні події в системі. Проілюструємо процес налаштування оповіщень, використовуючи інструмент Saved Search.

Здійснюємо пошук подій за значенням поля пріоритет (поєднує у собі інформацію про джерело події та її важливість) syslog.priority: ”10”, та використовуємо фільтрацію результатів за параметрами: додаток-джерело події та рівень важливості «Critical» (рис. 4).

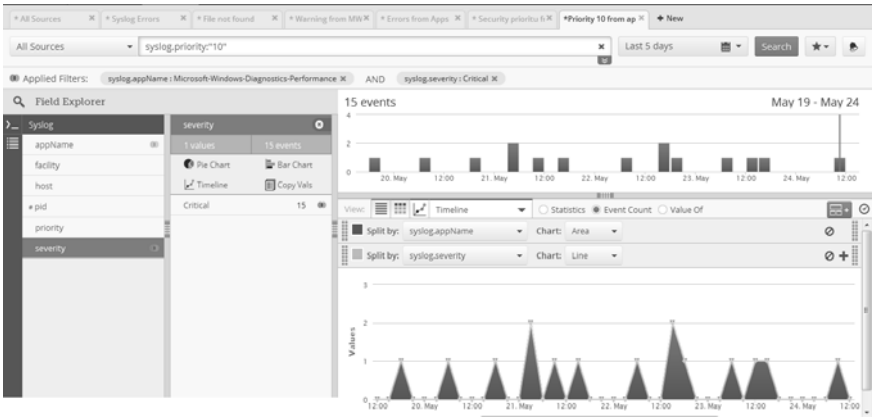

Рис. 4. Результати пошуку за значенням
поля та фільтрами із параметрами

Збережемо даний пошук для подальшого використання. Можна створити та зберігати необмежену кількість контекстних пошуків, використовуючи інструмент Saved search (рис. 5).

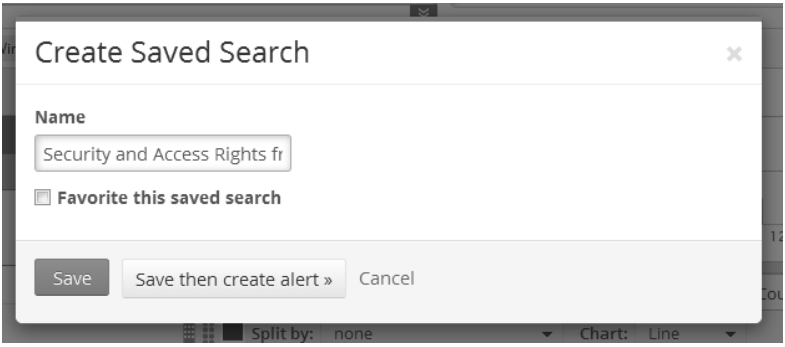

Рис. 5. Використання інструменту Saved Search

Натиснувши Save then create alert, створимо оповіщення за даними параметрами пошуку (рис. 6).

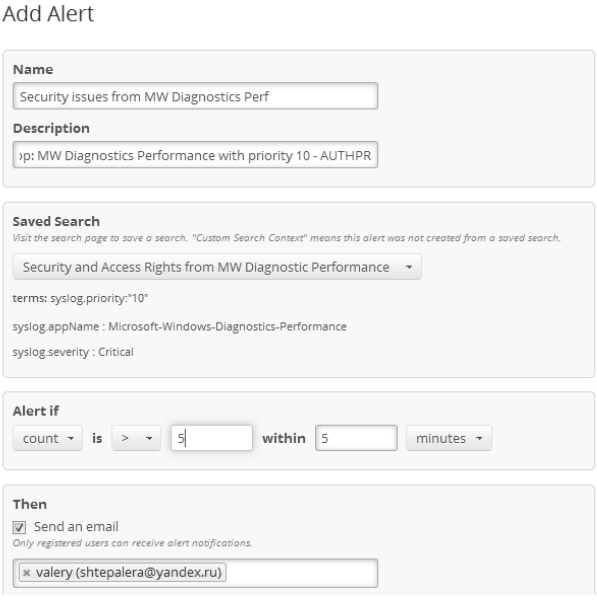

Рис. 6. Створення оповіщення «Security issues from MW Diagnostics Performance»

У вікні налаштування параметрів оповіщення заповнюємо поля Name (Назва) та Description (Опис). Далі наведено параметри збереженого пошуку, на основі якого формується оповіщення.

В області форми Alert if задаємо кількість подій, які відповідають умовам пошуку, та часовий проміжок для активації функції оповіщення.

Далі обираємо e-mail (наприклад, поштова адреса адміністратора мережі), на який дане оповіщення необхідно надіслати. Також можливим є отримання оповіщень через Pager Duty та чат-сервіси HipChat або Slack.

Активуємо оповіщення (Enable this alert) та зберігаємо.

Перейшовши до розділу Alerts на верхній панелі, можемо переглянути весь список створених оповіщень (рис. 7).

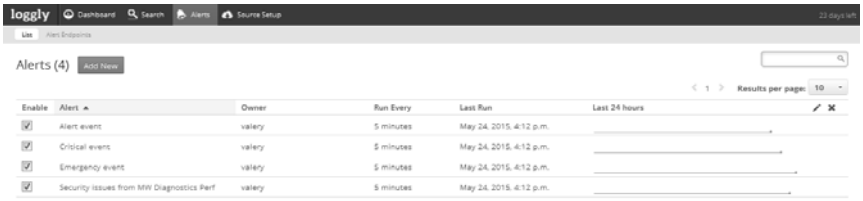

Рис. 7. Перелік оповіщень про критичні події

Таким чином, дослідивши основні інструменти сервісу Loggly, переконалися, що вони дозволяють зручно організувати збір логів системи та додатків від різних джерел, нормалізувати лог-дані та їх аналізувати.

Розглянемо питання безпеки даних, які відправляються до Loggly. Відомо, що існує кілька способів для безпечної відправки даних до хмарного сервісу Loggly: механізм доставки для Syslog, який забезпечує безпеку на транспортному рівні (TLS), HTTPS — розширення протоколу HTTP, що підтримує шифрування. Дані, які передаються за протоколом HTTPS, «упаковуються» в криптографічний протокол SSL або TLS.

Дані зберігаються в центрах обробки даних, які сертифіковані ISO & SOC2. При отриманні даних Loggly, всі взаємодії здійснюються в рамках безпечних сесій (HTTPS), зашифрованих у протокол Secure Sockets Layer (SSL).

Тарифи та умови використання хмарного сервісу Loggly.

Кожна компанія може обрати зручний для себе тарифний план залежно від:

- щоденного обсягу лог-данних, що необхідно обробляти;

- строку зберігання даних.

Для користувачів пропонується чотири тарифних плану: «Lite — Free Forever Plan», «Standard», «Pro», «Enterprise». Детальнуа інформацію по кожному тарифному плану наведено в табл. 2.

Таблиця 2

ТАРИФИ НА ВИКОРИСТАННЯ ХМАРНОГО СЕРВІСУ LOGGLY

Назва тарифу	Умови	Щоденний обсяг лог-даних	Строк зберігання даних	Ціна
Lite — Free Forever Plan	Забезпечує централізований збір логів, користування функціями пошуку та фільтрації даних, робочий простір лише для 1 користувача аканту	200 Мб	7 днів	Безкоштовно
Standard	Використання додатків з невеликим об'ємом лог-даних	1 Гб	7 днів	$49 на місяць
Pro	Використання виробничих додатків із кількома користувачами, великим об'ємом даних і необхідністю періодичного архівації	Від 1 Гб до 100 Гб	Від 15 днів до 90 днів	Від $109 до $5100 на місяць
Enterprise	Використання великомасштабних виробничих додатків із розподіленими командами користувачів і вимогами тривалого зберігання даних	Від 150 Гб до 200 Гб	Від 90 днів	Визначається індивідуально з відділом продажів

Тарифний план «Pro» та «Enterprise» дозволяють здійснювати архівацію даних до Amazon Simple Storage Service (Amazon S3) — он-лайн веб-служба, яка надає можливість зберігання та отримання будь-якого обсягу даних, у будь-який час з будь-якої точки мережі.

Після реєстрації компанії надається безкоштовний 30-денний період користування сервісом Loggly. Протягом цього періоду у користувачів є можливість завантажувати необмежений об'єм лог-даних. Перейшовши до меню Profile — Overview можна побачити графік «Data Volume Usage», який надає інформацію про щоденний обсяг завантажених лог-даних на кожен день безкоштовного періоду користування сервісом. Використовуючи графік, можна визначити потреби компанії щодо обсягу аналізованих даних ій відповідно обрати тарифний план.

Отже, підсумуємо та зазначимо переваги використання сервісу Loggly для збору та аналізу даних лог-журналів:

1) збір логів без використання спеціальних агентів, які необхідно додатково встановлювати та оновлювати;

2) автоматизований «парсинг» — розбір подій, тобто можливість автоматичного вилучення окремих полів даних;

3) потужні можливості пошуку: повнотекстовий пошук, пошук за окремими полями, рядами і логічними змінними. Також забезпечується фільтрація даних за полями загальноприйнятих лог-форматів;

4) необмежена кількість збережених пошуків — будь-який контекстний пошук може бути збережений для подальшого використання;

5) функція побудови графіків «Point-and-click»: забезпечує можливість будувати графіки, лінійчаті діаграми, кругові діаграми, діаграми з областями на основі підрахунку сум, середніх, стандартних відхилень, обираючи параметри з випадаючих меню;

6) вбудована функція оповіщень дозволяє отримувати повідомлення на електронну пошту або ж такі чат-сервіси, як HipChat і Slack. Індивідуально регульовані «dashboards», які дозволяють розміщувати результати пошуків і графіків за бажанням користувача;

7) можливість додати необмежену кількість користувачів до власного аканту. Також можна визначити рівні доступу користувачів до журналів;

8) можливість надсилати необмежений об’єм лог-даних під час використання безкоштовної пробної версії;

9) гнучка цінова політика. Кожна компанія може обрати зручний для себе тарифний план залежно від щоденного об’єму аналізованих даних і строку зберігання даних.

Висновки. Якщо виявлена за допомогою сервісу Loggly подія інформаційної безпеки ідентифікується системним адміністратором або адміністратором безпеки як інцидент інформаційної безпеки, то дані про цю подію необхідно занести в Журнал інцидентів інформаційної безпеки.

До Журналу необхідно занести наступні дані про інцидент: тип інциденту; механізм реалізації інциденту; джерело загрози (зовнішнє/внутрішнє та тип; якщо джерелом загрози виявися працівник підприємства — вказати його посаду); кількість джерел загрози; активи підприємства, які опинились під загрозою; елементи інформаційної інфраструктури, які опинись під загрозою; тип інформації, яка опинилась під загрозою; властивості інформації, що були порушені; дата та час виявлення інциденту; місце виникнення інциденту; дата та час усунення інциденту; контактна

особа, яка виявила інцидент; контактна особа або служба, що усунула інцидент; заходи для усунення інциденту; примітки.

Далі системний адміністратор або адміністратор безпеки надсилає заявку до Центру інформаційної безпеки, використовуючи електронну пошту. У заявці необхідно вказати: тип інциденту; механізм реалізації інциденту; джерело загрози (зовнішнє/внутрішнє та тип; якщо джерелом загрози виявися працівник підприємства — вказати його посаду); кількість джерел загрози; активи підприємства, що опинились під загрозою; елементи інформаційної інфраструктури, що опинись під загрозою; тип інформації, що опинилась під загрозою; властивості інформації, що були порушені; дата та час виявлення інциденту; місце виникнення інциденту. В темі листа адміністратор вказує назву підприємства та групу, до якої воно відноситься.

Література

1. *Бєгун А. В.* Аналіз загроз інформації порталу через атаки на додатки // Моделювання та інформаційні системи в економіці. Міжвідомчий наук. збірник. Вип. №80. — К:. КНЕУ, 2009. — С.101–107.
2. *Галіцин В.К.* Системи моніторингу: Монографія. — К.: КНЕУ, 2000. — 231 с.
3. *Камінський О.Є.* Хмарні технології в парадигмі інформаційної економіки: монографія / О.Є. Камінський. — Київ: КНЕУ, 2018. — 230 с.
4. Biehun A., Ignatova Iu. Estimation the reliability of the elements of cloud services. //Operations Research and Decisions. — Wroclaw: Wroclaw University of Technology, 2017. — Vol. 27(3), — Pg. 65–80.

References

1. Biehun A. V. Analiz zagroz informaciyi portalu cherez ataky na dodatky [Analysis of portal information threats by attack on applications] // Modelyuvannya ta informacijni systemy v ekonomici. Mizhvidomchyj nauk. zbirnyk. Vol. № 80. — K. : KNEU, 2009. — S.101–107: [in Ukrainian].
2. Galicyn V.K. Systemy monitoryngu: Monografiya [Monitoring systems: Monograph]. — K.: KNEU, 2000. — 231 s: [in Ukrainian].
3. Kaminskyj O.Ye. Xmarni texnologiyi v paradygmi informacijnoyi ekonomiky: monografiya [Cloud technologies in the information economy paradigm: monograph] / O.Ye. Kaminskyj. — K.: KNEU, 2018. — 230 s: [in Ukrainian].
4. Biehun A., Ignatova Iu. Ocinka nadijnosti elementiv hmarnyh servisiv [Estimation the reliability of the elements of cloud services] //Operations Research and Decisions. — Wroclaw: Wroclaw University of Technology, 2017. — Vol. 27(3), — Pg. 65–80: [in English].

Статтю подано до редакції 30.10.2018 р.