УДК 621.391 к.т.н., с.н.с. **Міночкін Д.А.** (НТУУ «КПІ ім. Ігоря Сікорського»)
Нсер А.М. (НТУУ «КПІ ім. Ігоря Сікорського»)

DOI: https://doi.org/10.17721/2519-481X/2022/77-11

ПРОГРАМНІ МЕТОДИ МОНІТОРИНГУ МЕРЕЖЕВОЇ БЕЗПЕКИ

В роботі розглянуто програмні методи моніторингу мережевої безпеки (NSM - Network Security Monitoring). Із зростанням і швидким розвитком мобільного зв'язку, великих даних і технологій штучного інтелекту ми вступаємо в еру мобільного Інтернету. З безперервною інтелектуалізацією мережевої безпеки та інфраструктури інформаційних технологій, вони широко використовуються в галузі промислового контролю, що робить мережеву безпеку все більш відкритою. В даний час спостерігається зростання кількості інформаційних загроз та факторів, що призводять до нестабільного функціонування мереж передачі даних. Передумовами цього зростання є масовість застосування, ускладнення ієрархії обчислювальних мереж та збільшення їх структурної складності, збільшення гетерогенності програмних та апаратних засобів, ускладнення функціональності мережевих сервісів, що призводить до появи різноманітних вразливостей. У таких умовах розробка та вдосконалення способів виявлення інформаційних загроз набувають великої важливості. Одним із компонентів забезпечення інформаційного захисту мереж є програмні комплекси, призначені для виявлення шкідливої чи підозрілої активності – методи моніторингу мережевої безпеки (NSM). Методи моніторингу мережевої безпеки (NSM) використовуються для моніторингу та обміну даними по мережі щодо подій, пов'язаних з інформаційною безпекою.

У статті наведено визначення методів моніторингу мережевої безпеки, їх класифікація, цикл NSM та їх опис. Розглянуто деякі з найвідоміших і широко використовуваних багатомодульних рішень NSM. Найвідомішими прикладами таких комбінацій є IDS/IPS, SEM/SIEM і UTM. Моніторинг мережевої безпеки перевіряє, чи працюють перші лінії захисту, надає можливість усунути загрози, перш ніж вони завдадуть реальної шкоди. Якщо в системі є вразливість, NSM дозволяє зрозуміти, де ці вразливості та як запобігти атакам.

Ключові слова: NSM, Network Security Monitoring, програмні методи моніторингу мережевої безпеки.

Вступ. На сьогодні більшість зусиль у сфері мережевої безпеки зосереджені на запобіганні атакам, однак рішення та методи, засновані на виявленні та реагуванні, набувають все більшої актуальності [1, 2]. У спільноті безпеки інформаційних технологій (IT) існує загальне переконання, що зловмисники рано чи пізно перевершують заходи профілактики. У цей момент необхідно застосувати механізми виявлення та реагування [3]. Моніторинг безпеки мережі (NSM) є одним із найкращих підходів до безпеки мережі [4].

Метою NSM є моніторинг стану даної мережі для виявлення аномальних подій і, якщо вони виявлені, для своєчасної реакції на них. Це серйозний виклик, оскільки комунікаційні мережі виробляють величезний обсяг даних з високою швидкістю, відповідно до визначення проблеми Big data [5]. Це ще складніше завдання, якщо взяти до уваги поширеність нових сценаріїв використання мережі, таких як 5G та IoT, або адаптацію до нових мережевих технологій (наприклад, SDN) [6, 7].

Аналіз останніх досліджень та публікацій. В літературі та дослідженнях розглядаються різні інструменти безпеки мережі, які реалізують декілька модулів NSM. А саме системи виявлення вторгнень (IDS) / системи запобігання вторгненням (IPS), системи керування подіями безпеки (SEM) / системи керування інформацією та подіями безпеки (SIEM), універсальний контроль загроз (UTM) і колекції інструментів; включаючи приклади як відкритих, так і комерційних рішень [8]. Однак, більшість досліджень присвячені лише певним типам загроз, заснованим на рішенні вузького спектру задачах безпеки мережі. Актуальним лишається створення методу, який зможе протистояти декільком загрозам одночасно та буде більш універсальним до більшості методів атак. Пропонується

використовувати існуючі методи та інструменти у взаємодії один з одним, таким чином створюючи потужну та масштабовану архітектуру для виявлення інцидентів.

Мета статті. Метою статті є наведення програмних методів моніторингу мережевої безпеки (NSM).

Виклад основного матеріалу. NSM - це збір, виявлення та аналіз даних безпеки мережі. Інформаційна безпека традиційно поділяється на багато різних типів, але відповідно до DoD 8500.2.1 [9] їх можна класифікувати наступним чином:

1. Захист. Даний тип зосереджується на захисті систем, щоб запобігти несанкціонованому використанню та вторгненню. Деякі з функцій, які зазвичай виконуються в цьому типі, включають оцінку вразливості, оцінку ризиків, керування захистом від шкідливих програм, навчання користувачів та інші загальні завдання забезпечення інформаційної безпеки.

2. Виявлення. Цей тип зосереджений на виявленні вторгнень, які активно відбуваються або мали місце раніше. Воно включає в себе моніторинг безпеки мережі та виявлення і попередження атак.

3. Відповідь. Третій тип зосереджений на відповіді після виявлення. Це включає стримування інцидентів, криміналістику мережі та хостів, аналіз зловмисного програмного забезпечення та звітування про інциденти.

4. Підтримка. Останній тип відповідає за керування людьми, процесами та технологіями, пов'язаними з інформаційною безпекою. Це включає укладання контрактів, підбір персоналу та навчання, розробку та впровадження технологій, а також управління системами підтримки.

Цикл NSM складається з трьох окремих фаз: збір даних, виявлення та аналіз (Рис.1.) [10].

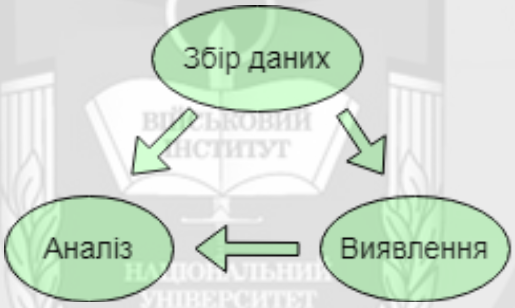

Рисунок 1 – Фази NSM

Цикл NSM починається з найважливішого етапу – збору даних. Збір даних відбувається за допомогою апаратного та програмного забезпечення, яке використовується для генерування, упорядкування та зберігання даних для подальшого виявлення та аналізу. Збір даних є найважливішою частиною циклу, оскільки вжиті кроки формують здатність організації виконувати ефективне виявлення та аналіз. Є кілька типів даних NSM і кілька способів їх збору. Найпоширеніші категорії даних NSM включають повні дані вмісту, дані сеансу, статистичні дані, дані пакетів і дані оповіщення. Залежно від потреб організації, архітектури мережі та доступних ресурсів ці типи даних можуть використовуватися переважно для виявлення. Спочатку збір даних може бути однією з найбільш трудомістких частин циклу NSM через кількість необхідних людських ресурсів. Ефективний збір даних вимагає узгоджених зусиль керівництва організації, команди з інформаційної безпеки та груп адміністрування мережі та систем. Збір даних включає такі завдання, як:

1. Визначення того, де в організації існує найбільший ризик
2. Виявлення загроз
3. Виявлення відповідних джерел даних
4. Уточнення частин збору джерел даних
5. Налаштування портів SPAN для збору пакетних даних
6. Створення сховища SAN для зберігання даних

7. Налаштування апаратного та програмного забезпечення збору даних.

Виявлення – це процес, за допомогою якого перевіряються зібрані дані та генеруються сповіщення на основі спостережених подій і аномальних даних. Зазвичай це робиться за допомогою певної форми сигнатури, аномалії або на основі статистики. Це призводить до створення даних сповіщення. Незважаючи на те, що основна частина виявлення виконується програмним забезпеченням, деяке виявлення відбувається шляхом ручного аналізу джерел даних. Особливо це стосується ретроспективного аналізу.

Аналіз є завершальним етапом циклу NSM, і він відбувається, коли людина інтерпретує та досліджує дані. Це часто включатиме збір додаткових дослідницьких даних з інших джерел, дослідження розвідувальних даних із відкритим кодом (OSINT), пов'язаних із типом сповіщення, створеного механізмом виявлення, та проведення OSINT-досліджень[11], пов'язаних із будь-якими потенційно ворожими хостами. Існує безліч способів проведення аналізу, але це може включати такі завдання, як:

1. Аналіз пакетів
2. Криміналістична експертиза мережі
3. Криміналістична експертиза хосту
4. Аналіз шкідливого програмного забезпечення

Системи виявлення вторгнень (IDS – Intrusion Detection Systems) є одними з найбільш використовуваних засобів безпеки. Вони в основному складаються з датчика, аналізатора та механізму виявлення. Якщо ці системи також дозволяють розгортати захисну відповідь на атаки вони називаються системами запобігання вторгненням (IPS – Intrusion Prevention Systems). Деякі з IDS еволюціонували до систем керування подіями безпеки (SEM – Security Event Management), які включають модуль інтегратора для покращення можливостей виявлення шляхом збору даних із різних джерел [12].

IDS – це системи, які реалізують набір методів для виявлення підозрілих дій (потенційних вторгнень) шляхом моніторингу та аналізу подій у мережі чи пристрої [12, 13]. Вони класифікуються як Host IDS (HIDS) і Network IDS (NIDS) відповідно до походження зібраних даних [13, 14]. HIDS розгортаються в кінцевих системах (хостах) і відстежують активність користувачів і поведінку внутрішніх процесів. NIDS спочатку збирають дані з мережі за допомогою датчиків мережевого трафіку; потім вони аналізують дані, щоб виявити порушення безпеки. Незалежно від типу IDS, коли дані отримані та ідентифіковані як (потенційно) шкідливі, система сповіщає операторів безпеки. Оскільки найвідоміші IDS є відкритими, ми розглядаємо лише цю категорію.

Snort це найпопулярніший IDS, його також можна використовувати як сніфер [13]. Snort - це NIDS на основі сигнатур, який дозволяє сканувати порти, а також реєструвати та сповіщати про будь-яку визначену аномалію. В останніх випусках цей IDS також дозволяє визначати базові відповіді у формі правил, які дозволяють блокувати мережевий трафік, пов'язаний із даним сповіщенням. Unified2 - це вихідний формат журналу, створений Snort. Реєстрація може генеруватися в трьох режимах: реєстрація пакетів, реєстрація попереджень і справжня уніфікована реєстрація. Журналювання пакетів використовується для захоплення пакетів, тоді як журнал попереджень реєструє лише події IT-безпеки. Справжнє уніфіковане журналювання дозволяє записувати як події, так і пакети.

Suricata - це мережева IDS у реальному часі та мережева IPS. Він відстежує мережевий трафік і виконує офлайн-обробку файлів pcap. Suricata базується на підписах і надає вивід у стандартних форматах, таких як YAML або JSON, але його також можна налаштувати для створення журналів у Unified2 [15].

OSSEC - це HIDS з відкритим кодом, який виконує аналіз журналів, перевірку цілісності, моніторинг записів Windows і виявлення руткітів. Крім того, OSSEC надає сповіщення та зберігає копії змінених файлів. Це також дозволяє налаштувати правила брандмауера для блокування зловмисного мережевого трафіку, включаючи певні IP-адреси. OSSEC є мультиплатформенним, оскільки його можна використовувати в більшості операційних систем. Незважаючи на те, що цей механізм має деякі функції SIEM, такі як можливість

кореляції журналів з кількох пристроїв і форматів, а також механізми для відповідності політикам безпеки, він традиційно вважається IDS [16].

Система управління подіями безпеки (SEM – Security Event Management) відповідає за збір, аналіз і посилення індикацій і попереджень для виявлення та реагування на вторгнення. Його метою є візуалізація та розуміння мережевих даних за допомогою єдиного уніфікованого інструменту, який поєднує різні джерела даних. З цією метою SEM дозволяє перемикатися між різними джерелами даних для проведення аналізу даних, що значно скорочує час, необхідний для розслідування інциденту безпеки (особливо якщо звітування здійснюється за допомогою графічних засобів). Однією з особливостей, яка робить систему SEM таким потужним інструментом, є те, що вона дозволяє візуалізувати та пріоритезувати події, таким чином допомагаючи операторам служби безпеки інтерпретувати та розуміти сигнали тривоги [13].

Систему безпеки та управління подіями (SIEM – Security Information and Event Management) можна описати відповідно до визначення Gartner [17] як систему, яка «аналізує дані про події в режимі реального часу для раннього виявлення цілеспрямованих атак і витоку даних, а також збирає, зберігає, розслідує та звітує про дані в журнал для реагування на інциденти». Системи SIEM - це комбінація двох різних систем: SEM і систем керування інформацією про безпеку (SIM). Основна відмінність від SEM полягає в тому, що SIEM також створює звіти та включає функції для відповідності нормативним вимогам, тоді як SEM не обов'язково цього робити (насправді, це функція, яка зазвичай надається модулем SIM). SIEM є найпопулярнішим (і дорогим) типом систем інтеграції в галузі.

Zeek був розроблений Верном Паксоном і Робіном Соммером як дослідницька робота. Зараз він еволюціонував і широко використовується компаніями, а також дослідницькими та освітніми організаціями [18]. Це повний інструмент з відкритим кодом для NSM, який дозволяє як виявляти аномалії, так і виявляти інциденти на основі сигнатур [12, 18]. Zeek збирає мережевий трафік за допомогою libpcap. Потім механізм подій обробляє дані, виконуючи пасивний аналіз таких даних. Це також дозволяє збирати й аналізувати сеанси певних служб. Крім того, Zeek можна запрограмувати на виконання дій при оцінці подій (наприклад, на виконання програми для забезпечення активної реакції на виявлену подію).

Prelude це SIEM для Linux, який збирає, поєднує та контролює події безпеки. Prelude реалізує стандартний формат IDMEF (RFC 4765) як частину компонента синтаксичного аналізу, щоб він міг читати широкий спектр форматів журналів [19]. Крім того, він створює звіти про події. Його інтерфейс забезпечує криміналістичний режим, який дозволяє досліджувати дані за великі періоди. Цей SIEM можна використовувати в комерційній версії, ціни на яку налаштовуються для кожної організації та залежать від обсягу заходів.

Wazuh - це SIEM для виявлення вторгнень на основі сигнатур, який був розроблений одноіменною компанією [20]. Wazuh базується в OSSEC і використовується в поєднанні з Elastic Stack. Це дозволяє контролювати систему для аналізу безпеки, виявлення вторгнень і вразливостей. Крім того, Wazuh забезпечує реагування на інциденти безпеки, включаючи цілісність і відповідність [20]. Завдяки функціям Elastic Stack реалізовано компонент парсингу.

OSSIM (Open Source Security Information Management) - це SIEM, розроблений компанією Alien Vault (AT&T Cybersecurity з лютого 2019 року) [21], і він використовує модуль аналізу загроз Open Threat Exchange (OTX), який дозволяє користувачам вносити та отримувати оновлену інформацію про безпеку в режимі реального часу. Можливості OSSIM включають виявлення активів, оцінку вразливостей, виявлення вторгнень, моніторинг поведінки та кореляцію подій. Він інтегрує різні програмні модулі, щоб забезпечити повне рішення NSM. Серед інших інструментів це рішення включає як хост, так і мережевий IDS. Частина NIDS забезпечує виявлення вторгнень і сканування мережевого трафіку. Він також шукає сигнатури останніх атак, а також зловмисне програмне забезпечення або інші можливі способи спроб скомпрометувати систему. HIDS аналізує поведінку та стан системи, сповіщаючи, коли підозрює, що щось не так. Подібно до інших SIEM, OSSIM дозволяє виявляти та пріоритезувати найважливіші загрози та аномалії.

UTM – це тип багатофункціонального продукту мережевої безпеки, який використовується малим і середнім бізнесом [22]. Ці пристрої мають функціональні можливості високого рівня (багатофункціональний шлюз), якими можуть бути, наприклад, брандмауер на прикладному рівні моделей TCP/IP та OSI, запобігання та виявлення вторгнень (IPS та IDS), антивірус, захист від спаму та антифішинг. Основними перевагами UTM є їх низька вартість і складність, а недоліками є те, що UTM зазвичай мають обмежену потужність обробки, і вони не можуть корелювати події. Оскільки це апаратне рішення, неможливо знайти реалізації з відкритим кодом. Таким чином, ми включаємо лише комерційні інструменти в цій частині огляду.

Barracuda CloudGen Firewall - комерційний UTM, який забезпечує виявлення вторгнень і захист. CloudGen Firewall також захищає від відомих атак, таких як відмова в обслуговуванні (DoS) або ботнет-атаки. Крім того, це рішення забезпечує автентифікацію та підключення до VPN. Його брандмауер дозволяє перевіряти та фільтрувати пакети [23].

WatchGuard - комерційний UTM, який забезпечує виявлення вторгнень і захист. WatchGuard корелює дані з різних джерел, що покращує його здатність виявляти загрози та реагувати на них, а також генерувати звіти. Крім того, він забезпечує антивірусні функції та контроль програм, який пов'язаний з поведінкою користувача. WatchGuard пропонує розширений блокувальник постійних загроз, який дозволяє виявляти складні атаки, такі як програми-вимагачі, і діяти проти них; а також має функцію запобігання спаму [25].

Sophos - комерційний UTM, який забезпечує виявлення вторгнень і захист. Sophos дозволяє виявляти загрози та діяти проти них. Коли Sophos виявляє заражену систему, вона ізолює цю систему. Крім того, він надає механізми віддаленого доступу, такі як VPN. Це рішення також включає розширений брандмауер для моніторингу даних трафіку та функції захисту від спаму [26]. Sophos класифікується як лідер у Gartner's Magic Quadrant у 2018 році [24].

Колекції інструментів - це інструменти мережевої безпеки, які складаються з низки різнорідних програмних рішень. Крім того, оскільки вони є з відкритим кодом, вони постійно розвиваються.

Sguil — це набір інструментів з відкритим кодом для моніторингу безпеки мережі, який дозволяє збирати, аналізувати, сповіщати та реагувати на вторгнення. Sguil надає інтерфейс реального часу та включає два IDS. Деякі інструменти з набору Sguil: [27]:

1.MySQL, як служба бази даних.

2. Snort і Suricata для виявлення та сканування вторгнень у мережу, а також для реєстрації пакетів і вирішення інцидентів.

3. Tcpdump, для збору мережевого трафіку з журналів пакетів.

4. Wireshark для аналізу зібраних пакетів.

Security Onion - це набір інструментів з відкритим кодом, який надається як дистрибутив Linux. Security Onion дозволяє відстежувати, записувати та керувати журналами, а також виконувати виявлення вторгнень і реагувати на інциденти безпеки IT. Він реалізує всі модулі NSM. Деякі інструменти з набору Security Onion [28]:

5. Elastic Stack і Logstash, як механізм пошуку та аналізу, який також перетворює та централізує дані, забезпечуючи функціональні можливості візуалізаці.

6. Snort, Suricata та Zeek для виявлення мережевих вторгнень, сканування та видачі сповіщень, а також для реєстрації пакетів.

7. Wazuh, для виявлення вторгнень на хост.

8. Sguil для моніторингу безпеки мережі та аналізу приводу подій.

9. Squert для перегляду та візуалізації даних Sguil.

10. Cyberchef для шифрування, стиснення та аналізу даних.

11. NetworkMiner, для криміналістичного аналізу.

Журнали брандмауера є одним із найкорисніших джерел даних безпеки, оскільки вони надають інформацію про кожен доступ (невдалий чи успішний, авторизований чи ні) до

мережі. Однією з головних переваг брандмауерів є те, що їх можна знайти в будь-якій мережі. Наприклад, Windows Defender в операційних системах Windows 10, але є також вдосконалені брандмауери, такі як Sophos, які фактично включені в рішення UTM.

Інструменти оцінки вразливостей запускаються в мережі та кінцевих системах. Ці інструменти виявляють слабкі місця та діри в безпеці, які можуть уможливити несанкціонований доступ до системи. Двома добре відомими інструментами для цієї мети є Nmap і Nessus. Nmap (Network Mapper) - це програма з відкритим кодом для сканування портів для оцінки безпеки операційних систем, що дозволяє виявляти вразливості та надавати корисну інформацію про відкриті порти та служби. Хоча спочатку Nmap розроблявся для Linux, тепер він є мультиплатформенним. Nessus також є багатоплатформною програмою для сканування вразливостей в операційних системах. Спочатку Nessus був з відкритим вихідним кодом, але тепер це приватне програмне забезпечення (хоча існують альтернативи з відкритим кодом, такі як OpenVAS (Open Vulnerability Assessment Scanner)). Аналіз оцінки вразливості зазвичай починається зі сканування портів, яке можна зробити, наприклад, за допомогою Nmap. Після виявлення відкритих портів Nessus надсилає кілька запитів проти таких портів, щоб виявити наявні вразливості. Результати можна експортувати в різні формати, такі як простий текст або XML. Іншими корисними ресурсами, які дозволяють отримати дані про вразливості, є національна база даних вразливостей (NVD – National Vulnerability Database) і бази даних загальних вразливостей (CVE – Common Vulnerabilities and Exposures). NVD - це державна служба, яка надається Національним інститутом стандартів і технологій США (NIST) для перерахування та класифікації існуючих уразливостей у поточному програмному та апаратному забезпеченні [29]. CVE - ще одна подібна послуга, що надається MITRE6, яка також включає NVD. Ці бази даних пропонують найновішу інформацію про відомі вразливості в операційних системах і програмах/службах, а також про їх вирішення (якщо відомо). Уразливості зазвичай виявляють за допомогою будь-якого з вищезгаданих або подібних інструментів.

Системи FIM дозволяють виявляти зміни у файлах, що зберігаються на пристроях, відносно базової копії таких файлів. Деякі з параметрів, які перевіряє FIM, це: дата модифікації/створення, дозволи на доступ і модифікацію, і контрольна сума (хеш) вмісту. Однією з проблем цього типу джерела даних є величезний обсяг даних і кількість помилкових спрацьовувань, які вони, як правило, генерують. Одним із інструментів, який реалізує можливості FIM, є OSSEC.

Threat Intelligence – це механізм, схожий на соціальну мережу або канали RSS, який дозволяє користувачам отримувати оновлену інформацію про загрози безпеці та/або проблеми. Це дозволяє обмінюватися корисною інформацією про безпеку між організаціями, що також може бути корисним для вдосконалення механізмів виявлення. Наприклад, якщо організація виявляє нову атаку, решта організацій, які використовують аналіз загроз, отримують інформацію, що дозволяє їм запобігти атаці або боротися з нею більш ефективним способом. Крім того, Threat Intelligence використовує знання, пов’язані з організацією, включаючи контекст або індикатори ризику, а також наявні звіти про попередні атаки, серед інших даних [30]. Мета використання інформації від організації полягає в тому, щоб передбачити загрози на основі попереднього досвіду, беручи до уваги загрози як внутрішніх, так і зовнішніх організацій. Інструменти Threat Intelligence відповідають за збір цієї інформації та створення звітів, які можна інтегрувати з іншими механізмами безпеки, такими як системи SIEM. Threat connect і Cyber Threat Alliance є двома комерційними інструментами для аналізу загроз, тоді як Open Threat Intelligence і Collective Intelligent Framework є прикладами рішень з відкритим кодом.

Висновки. У цій статті було розглянуто сучасний стан моніторингу безпеки мережі (NSM), надано загальне розуміння та уніфіковану класифікацію його основних компонентів. Розглянуто програмні багатомодульні рішення, проаналізовано деякі інструменти безпеки мережі, які реалізують декілька модулів NSM. А саме системи виявлення вторгнень (IDS) / системам запобігання вторгненням (IPS), системам керування подіями безпеки (SEM) / системам керування інформацією та подіями безпеки (SIEM), універсальний контроль загроз (UTM) і колекції інструментів; включаючи приклади як відкритих, так і комерційних рішень. Ці модулі можна комбінувати різними способами, створюючи потужну та масштабовану архітектуру для виявлення інцидентів. Висвітлено сильні та слабкі сторони визначених модулів. Було розглянуто деякі з найвідоміших і широко використовуваних багатомодульних рішень NSM. Найвідомішими прикладами таких комбінацій є IDS/IPS, SEM/SIEM і UTM. Серед SIEM систем у плані функціоналу немає рішень, що явно виділяються. Однак системи Prelude та OSSIM добре підходять лише для невеликих мереж, у той час як OSSEC не має проблем із продуктивністю при використанні у великих проектах. Узагальнено відкриті питання та майбутні дослідницькі інтереси для кожного з модулів NSM. Таким чином, ландшафт безпеки як для традиційних, так і для сучасних мереж виграє від проектування систем, які включають усі визначені компоненти та комбінація різних систем багатомодульних рішень. Ба більше, все ще необхідно надавати ефективні рішення, які враховують обмежені ресурси, а також покращують стійкість у критичних інфраструктурах.

REFERENCES:

1. Samson R., (2020) “Prevention vs DetectionBased Security Approach,” Clearnetwork, www.clearnetwork.com/prevention-vsdetection-cybersecurity-approach/, *Tech. Rep*.,
2. Rapid7, (2015) “Prevention vs Detection, Rebalancing Your Security Program,” www.rapid7.com/resources/prevention-vsdetection/
3. Comodo, (2020) “Advanced Threat Protection: Security Incident Response Tools,”, *Tech. Rep.*
4. Bejtlich, R. (2005) The TAO of the Network Security Monitoring. Beyond Intrusion Detection.
5. Camacho, J. Maciá-Fernández, G. Verdejo, J. E. D. and García-Teodoro, P. (2014) “Tackling the Big Data 4 Vs for Anomaly Detection,” *INFOCOM’2014 Workshop on Security and Privacy in Big Data*, pp. 500–505
6. X. Ji, K. Huang, L. Jin, H. Tang, C. Liu, Z. Zhong, W. You, X. Xu, H. Zhao, J. Wu, and M. Yi, (2018) “Overview of 5G security technology,” Science China Information Sciences, vol. 61, no. 8, pp. 1869–1919,.
7. Thudumu, S. Branch, P. Jin, J. and Singh, J. J. “A comprehensive survey of anomaly detection techniques for high dimensional big data,” vol. 7, no. 1.
8. Fuentes-García, M. Camacho, J. and Maciá-Fernández, G. “Present and Future of Network Security Monitoring” 10.1109/access.2017.doi
9. US Department of Defense Instruction 8500.2, (2003) “Information Assurance (IA) Implementation” http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf.
10. Sanders, C. (2014). “The Practice of Applied Network Security Monitoring. Applied Network Security Monitoring”, 1–24. doi:10.1016/b978-0-12-417208-1.00001-5
11. Dokman, T. Ivanjko, T. (2020). “Open Source Intelligence (OSINT): issues and trends”. doi:10.17234/infuture.2019.23
12. Collins, M. “Network Security Through Data Analysis. Building situational awareness”, *O. Media, Ed. O’Reilly*, 2014.

13. INCIBE, (2017) “Diseño y Configuración de IPS, IDSy SIEM en Sistemas de Control Industrial,” https://www.incibe-cert.es/blog/diseno-yconfiguracion-ips-ids-y-siem-sistemas-controlindustrial

14. Alpcan, T. and Basar, T. (2011) “Network Security. A Decision and Game-Theoretic Approach”. *Cambridge University Press*

15. ATT Cybersecurity, (2020) “Suricata IDS: an overview of threading capabilities,” https://cutt.ly/jyZbAeI, *Tech. Rep*.

16. OSSEC Project Team,(2008) “Open Source HIDS SECurity,” https://www.ossec.net/

17. Gartner, (2019) “What is Security Information and Event Management (SIEM)?” https://www.gartner.com/reviews/market/securityinformation-event-management

18. Paxson, V. and Sommer, R. “The Zeek Network Security Monitor (Bro),” https://www.zeek.org/

19. Prelude, (2020) “PRELUDE SIEM. Smart Security,” https://cutt.ly/bfTTiuN

20. Wazuh Inc., (2019) “The Open Source Security Platform,” https://wazuh.com/

21. AT&T-cybersecurity,(2019) “AlienVault(R) Unified Security Management(R) (USM),” https://www.alienvault.com/products

22. Gartner, (2019) “Unified Threat Management (utm)” https://www.gartner.com/en/informationtechnology/glossary/unified-threat-management-utm

23. Barracuda, (2020) “Barracuda CloudGen Firewall,” https://cutt.ly/FgefB

24. BAKOTECH, (2018) “WatchGuard UTM is Recognized the Only Visionary in the Gartner Magic Quadrant for the 4th Time,” https://bit.ly/3aNkYO8

25. WatchGuard, (2020) “WatchGuard Security Services,” https://www.watchguard.com/wgrdproducts/security-services

26. Sophos, (2020) “The world’s best visibility, protection, and response,” https://www.sophos.com/enus/products/next-gen-firewall.aspx

27. Visscher, B. (2014) “Sguil,” https://sourceforge.net/projects/sguil/

28. Security Onion Solutions, (2008) “Security Onion,”https://securityonion.net/

29. National Institute of Standards and Technology (NIST), (2019) “National Vulnerability Database (NVD),” https://nvd.nist.gov/

30. Molina, J. (2016) “Threat Intelligence: el porqué de las cosas,” https://www.welivesecurity.com/laes/2016/12/01/threat-intelligence/.

Ph. D. Minochkin D.A.,
Nser A.M.

SOFTWARE METHODS OF NETWORK SECURITY MONITORING

The software methods for monitoring network security (NSM - Network Security Monitoring) are discussed. With the growth and rapid development of mobile communications, rich data and artificial intelligence technologies, we are entering the era of the mobile Internet. With the continuous intellectualization of network security and infrastructure, information technology is widely used in the field of industrial control, making network security more and more open, bringing a new network security control system to the traditional relatively closed industrial control system. Currently, there is an increase in the number of information threats and factors leading to the unstable operation of data transmission networks. The prerequisites for this growth are the mass application, the complication of the hierarchy of computer networks and the increase in their structural complexity, the increase in the heterogeneity of software and hardware, the complication of the functionality of network services, which leads to the emergence of various vulnerabilities. Under such conditions, the development and improvement of methods for identifying information threats are of great importance. One of the components of ensuring information protection of networks is software systems designed to detect harmful or suspicious activity - network security monitoring methods (NSM). Network security monitoring techniques (NSM) are used to monitor network

communications for information security events. For maximum effect, a combination of capturing the entire packet in addition to logging network activity is recommended.

This article provides definitions of network security monitoring methods, their classification, phases of the method cycle and their description. Some of the best known and widely used multi-module NSM solutions have been reviewed. The best known examples of such combinations are IDS/IPS, SEM/SIEM and UTM.

Network security monitoring is important because it checks if the first lines of defense are working, gives us the opportunity to eliminate threats before they cause real damage if there is a vulnerability somewhere in your system, and allows us to understand where these vulnerabilities are and how to fix them before something will happen.

Keywords: NSM, Network Security Monitoring, network security monitoring software methods.