Хоменко В. Р., здобувач,
Бродський Ю. Б., к.т.н., доцент,
Державний університет «Житомирська політехніка»

АВТОМАТИЗОВАНІ РІШЕННЯ FORTIGATE ДЛЯ АНАЛІЗУ ТРАФІКУ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У ХМАРНИХ СИСТЕМАХ

Хмарні середовища стають все більш популярними, але й більш складними. Це робить їх вразливими до кібератак. Моніторинг хмарної безпеки є ключовим компонентом для захисту хмарних ресурсів. Рішення FortiGate пропонують широкий спектр можливостей для моніторингу хмарної безпеки, які допомагають організаціям захистити свої дані та програми.

FortiGate є інтегрованою платформою забезпечення мережевої безпеки, яка пропонує широкий спектр функцій, спрямованих на захист мережі від різних видів загроз. Одним з ключових напрямків застосування FortiGate є моніторинг безпеки в хмарних середовищах.

Fortinet дозволяє організаціям модернізувати мережевий моніторинг за допомогою рішення FortiMonitor, яке є цифровою платформою моніторингу досвіду, яка надає групам мережевих операцій неперевершений рівень видимості.

FortiMonitor забезпечує безперебійну взаємодію між користувачами та їхніми програмами. Підприємства мають можливість корелювати телеметрію між пристроями кінцевих користувачів і мережами. Це покращує співпрацю між командами, такими як DevOps, ITOps, NetOps і служби підтримки, тому вони можуть реагувати на проблеми швидше та ефективніше.

FortiMonitor доступний організаціям як рішення SaaS для моніторингу їхніх хмарних програм, контейнерів, цифрового досвіду, інфраструктури та мереж [1].

Однією з переваг FortiGate є його інтеграція з іншими рішеннями безпеки, що дозволяє підвищити ефективність моніторингу та реагування на загрози. Наприклад, FortiGate може інтегруватися з системами моніторингу подій (SIEM), з системами виявлення вторгнень (IDS/IPS) чи з системами управління захистом інформації (IPS). Це дозволяє створити комплексну систему безпеки, яка забезпечує захист на всіх рівнях мережевої інфраструктури та дозволяє швидко реагувати на потенційні загрози.

Рішення FortiGate пропонують такі можливості моніторингу хмарної безпеки:

- Моніторинг журналів: FortiGate може збирати журнали з хмарних ресурсів, таких як віртуальні машини, контейнери та мережеві пристрої. Ці журнали можна використовувати для виявлення підозрілої активності та інцидентів безпеки.
- Моніторинг мережі: FortiGate може відстежувати мережевий трафік у хмарному середовищі. Це може допомогти виявити атаки, такі як DDoS-атаки та сканування портів.
- Моніторинг вразливостей: FortiGate може сканувати хмарні ресурси на наявність вразливостей. Це може допомогти організаціям усунути вразливості до того, як їх буде використано зловмисниками.
- Моніторинг відповідності: FortiGate може допомогти організаціям дотримуватися нормативних вимог, таких як GDPR [2].

FortiGate надає засоби для аудиту безпеки, що дозволяє проводити регулярні перевірки на предмет виявлення слабких місць та вразливостей у хмарній інфраструктурі. Це допомагає забезпечити відповідність з вимогами безпеки та захисту даних у хмарних середовищах.

Отже, інтеграція рішень FortiGate для моніторингу безпеки в хмарних обчисленнях може значно підвищити рівень безпеки та захисту інформації у сучасних організаціях. Їхні автоматизовані засоби аналізу трафіку та виявлення аномалій, спільно з інтеграцією з іншими системами безпеки та професійним персоналом, роблять FortiGate невід'ємною складовою захисту в хмарних середовищах.

Список використаних джерел

1. Network Monitoring Definition [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/network-monitoring
2. Application monitoring [Електронний ресурс] – Режим доступу: https://docs.fortinet.com/document/fortimonitor/24.1.0/user-guide/223793/application-monitoring