Гончаров М. В., магістрант, гр. КБм-22-1,
Єфіменко А. А., к.т.н., доц.,
зав. кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»

SIEM СИСТЕМА IBM QRADAR ЯК СКЛАДОВА SOC НАСТУПНОГО ПОКОЛІННЯ

Операційний центр безпеки (SOC, Security Operations Center) це централізована організаційна одиниця, яка залучає людей, процеси та технології для постійного спостереження та покращення заходів безпеки організації. Головними завданнями будь-якого SOC є запобігання, виявлення, аналіз та відповідь на інциденти кібербезпеки.

SIEM (Security Information & Event Management) система є однією доступних технологій SOC та є невід'ємною його складовою. Зазвичай її задачею є постійний моніторинг, виявлення та аналіз подій та інцидентів безпеки, однак сучасні SIEM-системи також пропонують можливість певною мірою відповідати на інциденти в режимі реального часу або після їх попереднього аналізу. Саме тому що SIEM-системи виконують велику частку завдань всього SOC, вибір належної SIEM-системи може бути нелегким завданням.

Згідно з дослідженнями консалтингової IT-фірми Gartner, «магічний квадрант» (рис.1) SIEM-систем за 2022 рік вказує на лідерство SIEM системи IBM QRadar. Ця система також отримала нагороду Customers' Choice 2021.

Рис.1. Magic Quadrant for SIEM – 2022

IBM QRadar може бути розгорнута на реальному обладнанні, в публічній/приватній хмарі чи гібридному середовищі, або реалізована у форматі cloud-native, як QRadar on Cloud (QROC). Додатково до QRadar, компанія IBM пропонує такі продукти безпеки:

1. QRadar Network Insights, QNI.
2. QRadar Vulnerability Manager.
3. QRadar XDR Connect.
4. QRadar SOAR.
5. QRadar Advisor with Watson.

QNI надає поглиблений аналіз трафіку 7 рівня OSI, що в свою чергу дозволяє виявляти фішингові атаки, бічний рух та витоки даних. QRadar Vulnerability Manager – це платформа сканування застосунків, систем та пристроїв всередині мережі на наявність вразливостей. QRadar XDR Connect – це Cloud-native рішення, яке вводить поняття Threat Intelligence та Threat Hunting у процеси SOC. QRadar SOAR – це система оркестрації та автоматизації реагування зменшує час вирішення інциденту до іноді декількох хвилин, а також в рази зменшує обсяг інформації з якою працюють аналітики та дає змогу повністю сфокусуватись на серйозних інцидентах. QRadar Advisor with Watson – це система ШІ IBM Watson, яка допомагає аналітикам при аналізі ризиків та інцидентів, сортуванні та реагуванні.

Ці та інші продукти, як от продукти від різних вендорів з відкритого маркетплейсу IBM X-Force App Exchange, легко з'єднуються та взаємодіють із самою SIEM-системою. Багато які з розширень контенту з тієї ж екосистеми дають змогу QRadar'у «розуміти» повідомлення журналів ОС та пристроїв більшості провідних вендорів та компаній.

Хоч Gartner і виділяє декілька недоліків IBM QRadar (серед яких велика комплексність початкового встановлення та низька гнучкість у плані додавання нових джерел даних), вони з лишком перевершуються спектром можливостей системи, її інноваційністю та ефективністю роботи з нею. Саме ці якості визначають подальший вектор розвитку SIEM-систем та по-справжньому виносять IBM QRadar на рівень складової SOC наступного покоління.

Список використаних джерел

1. Magic Quadrant for SIEM. Gartner. URL: https://www.gartner.com/doc/reprints?id=1-2BDGWSVV&ct=221011&st=sb.
2. Magic Quadrant Research Methodology. Gartner. URL: https://www.gartner.com/en/research/methodologies/magic-quadrants-research.

IBM Security QRadar SIEM – Overview. IBM. URL: https://www.ibm.com/products/qradar-siem.