UDC 004.056.5

G.E. Sagyndykova, S.A. Gnatyuk, Professor
(Satpayev University, Kazakhstan, Almaty)

Best Practices for Using New Rule Enhancement Models in SIEM

This article provides a brief overview and analysis of the SIEM system of the Qradar system, the principles of rules triggering rules and the correlation of events in the SIEM system of Qradar. Description and development of recommendations for the use of new models for improving rules in SIEM. Analysis and classification of events and incidents created on the basis of the study of network flows. Recommendations for developing and configuring rules for triggering and correlating information security events.

Introduction. Today, the SIEM system QRadar has become a popular and widespread solution not only for the financial and telecommunications sectors, but is also used in other areas, primarily in companies that have a lot of valuable data that needs to be protected from various threats. These are government agencies, financial, medical, trade, communications and transportation companies seeking to preserve their data for business continuity.

The rules for triggering in the SIEM system need constant revision and improvement, therefore the knowledge base obtained in the course of writing this article will be useful in practice for the information security community not only in Kazakhstan, but also in the CIS.

The main module of IBM QRadar is QRadar SIEM. This module is a system that collects, analyzes and manages events and network flows from devices, endpoints, servers, antiviruses, firewalls and various intrusion prevention systems.

QRadar SIEM centrally analyzes and consolidates collected data using Sense Analytics technology to identify deviations and complex security threats. This module collects all related events into one incident in order to provide IT professionals with detailed information about the attack, such as time, target, system vulnerabilities, user credentials, information about previous threats and intrusions.

QRadar SIEM can automatically detect data sources and also has built-in templates. This functionality makes it possible to implement the system as soon as possible. The management console is easy to use and provides a consolidated view of critical threat and vulnerability information. The advantage is that the control panel is provided as a functional, so users can create and customize their own workspace. The granularity of functionality makes it much easier to detect, select and analyze events and network flows that are directly related to violations.

The main element of IBM QRadar SIEM is a database that stores information about events and flows in the network. The system is equipped with DPI (deep packet inspection) technology, which collects events from firewalls and other network resources and performs in-depth analysis of network packets.

QRadar SIEM functionality also collects information about unauthorized user actions (for example, access to unauthorized resources, sending spam, clicking on phishing links) and network activity at the application level.

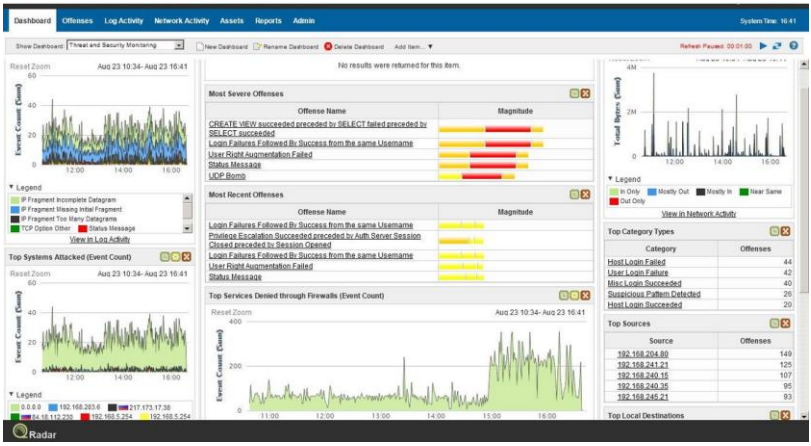

Figure 1 - Dashboard of the Qradar system

Functionality issues. Let's consider the above capabilities of IBM QRadar SIEM in more detail. Providing real-time visibility enables detection of application misuse, internal fraud, and small threats that could be overlooked among the millions of daily events. The solution enables collection of logs and events from a variety of sources, including security devices, operating systems, applications, databases, and access and identity management systems. Network flow data comes from switches and routers, including Layer 7 (application layer) data. It provides information from access and identity management systems and infrastructure services such as Dynamic Host Configuration Protocol (DHCP), as well as from network and application vulnerability scanners.

QRadar SIEM performs instant event normalization and correlation with other data for threat detection and regulatory reporting. The solution prioritizes events by highlighting a small number of real violations that pose the most serious business threat. The detected anomalies make it possible to identify changes in behavior associated with applications, computers, users and network segments. IBM X-Force Threat Intelligence software also detects suspicious IP address actions.

The solution enables you to more effectively manage threats by tracking serious incidents and providing links to all the required data for analysis. This allows you to detect activity outside of business hours or unusual use of apps and cloud services, as well as network activity that does not match saved usage patterns. To improve analytics, QRadar SIEM supports near real-time search in events and data streams, as well as in stored data. It is possible to perform unified searches in large distributed environments. For a deeper understanding and better display of applications, databases, collaboration products, and social media, you can use the IBM QRadar QFlow and IBM QRadar VFlow Collector devices, which enable detailed layer 7 network flow analysis.

The IBM QRadar advantage

Functionality is largely responsible for the key benefits for implementing IBM QRadar in an enterprise. The following advantages should be highlighted:

1. Simple configuration and deployment on-premises and in the cloud.

2. Displaying events in real time or based on the results of past periods.

3. Comprehensive incident detection and vulnerability management.

4. Strong analytical capabilities through which QRadar uses context for suspicious incidents, resulting in massive data reduction and faster incident detection rates.

5. Ability to provide analysis of behavior and deviations of network flow data and logs.

6. Stream data (network traffic) and event data are combined into a single dashboard, allowing users to accurately prioritize incident data, reducing false positives.

7. The IBM Security App Exchange enables customers, business partners, and other developers to create applications that extend the capabilities of QRadar.

8. Integrates with all related IBM products and many third party vendors.

The QRadar configuration panel allows you to schedule automatic system and device support updates, backup and restore, change the global system and management console settings, build a hierarchy of network segments, etc. User and role management allows you to flexibly configure the access rights of each user of the system to specific objects or reports.

The QRadar configuration panel allows you to schedule automatic system and device support updates, backup and restore, change global system and management console settings, build a hierarchy of network segments, etc.

User and role management allows you to flexibly configure the access rights of each user of the system to specific objects or reports.

Manage QRadar settings.

Using the Admin Tab QRadar is managed using the following functional elements, grouped by category:

-System Configuration — a category that combines system settings, accounting for installed licenses, auto-update, restore and backup, global notification system, management of users, their roles and authentication.

-Data Sources - a category that combines the setting of event sources, their extensions, grouping of event sources, configurable event properties, event storage settings, and various forwarding rules. It also contains settings for data streams sources, configurable properties of streams, settings for storing streams.

Administrator's Guide.

Remote Network sand Services Configuration category that combines settings for remote networks and services.

Plug-ins-category containing data on installed QRadar plug-ins and their corresponding settings.

Conclusion. An overview of working with a SIEM system is made, the functionality of the work, compatibility with other products is described, an administrator's guide is provided. IBM QRadar SIEM is one of the most effective security analytics systems. Importantly, the solution supports more than 200 products from leading manufacturers and collects, analyzes and correlates data across a wide range of systems, including networking, security, servers, hosts, operating systems and applications. In addition, an additional advantage of the solution is the low cost of the entry-level system.

References

1. Qradar [Electronic resource] - Access mode: URL: https://docplayer.ru/48200898-Sciencesoft-inc-rukovodstvo-administratora-qradar.html
2. SIEM Qradar [Electronic resource] - Access mode: URL: https://www.ibm.com/support/knowledgecenter/ru/SS42VS_7.3.3/com.ibm.qradar.doc/c_qradar_pdfs.html
3. Qradar system [Electronic resource] - Access mode: URL: https://ftpmirror.your.org/pub/misc/ftp.software.ibm.com/software/security/products/qradar/documents/7.3.0/ en / b_qradar_admin_guide.pdf
4. Qradar system [Electronic resource] - Access mode: URL: https://ict.moscow/presentation/primenenie-ibm-qradar-siem-v-rabote-ib/