

IBM QRadar vs. Splunk SIEM



About us

InfosecTrain is one of the finest Security and Technology Training and Consulting organization, focusing on a range of IT Security Trainings and Information Security Services. InfosecTrain was established in the year 2016 by a team of experienced and enthusiastic professionals, who have more than 15 years of industry experience. We provide professional training, certification & consulting services related to all areas of Information Technology and Cyber Security

What are SIEM and SOC?

Security Information and Event Management (SIEM) is the process of real-time analysis of security alerts generated by applications and network hardware, which is done by incorporating SIM and SEM under one framework. The machine-generated data is collected and monitored for security assessment.

SOC or the Security Operations Center is a facility that houses a team of security experts that monitors the organization's security and safeguards it. The SOC includes various sectors like SIEM, GRC, VAPT tools, IDS, and IPS. SIEM is an integral part of the Security Operation Center (SOC).

We will discuss two SIEM products here: Splunk and IBM QRadar.

Key Factors of Comparison

- History of Products
- Gartner's Magic Quadrant 2020
- Deployment & Target Industry
- Fundamental Comparison (Pricing, Metrics, and Intelligence)
- Pros and Cons of Splunk
- Pros and Cons of IBM QRadar

1. History of Products

Splunk: Splunk was founded in 2003, becoming the world's first, in the words of Splunk founders- "A Data-to-everything Platform," designed to bridge the gap between data and security by introducing the intelligent data monitoring system.

QRadar: Qradar was developed by Q1 Labs and acquired by IBM in 2011. IBM announced that the acquisition would help its clients more intelligently secure their organization by applying analytics to connect information from major security domains and forming security dashboards for their organizations.

2. Gartner's Magic Quadrant 2020:

Gartner is a prominent research and advisory company which has clients in 77% of the worlds' top 500 companies of all size. They release their research on the various domain of information security and Information technology on an annual basis, and we're considering one such annual summary. The image under discussion is the Gartner's Magic Quadrant for the year 2020 under the category of SIEM (Security Information and Event Management).

The quadrant is divided into four sections:

1. Challengers
2. Leaders
3. Niche Players
4. Visionaries

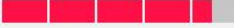
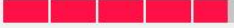
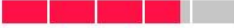
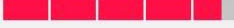


Gartner investigates various SIEM products on the basis of key attributes of comparison and importance and summarizes their report in the form of Magic Quadrant and Critical Capabilities.

Some of the attributes that Gartner evaluates the products are:

- Real-Time Monitoring
- Threat Intelligence
- Analytics
- Reviewer Demographics by Reviewer and Company Size

Below are the attributes used in QRadar v/s Splunk for this year.

	 IBM	 Splunk
Threat Intelligence	 4.4 (105)	 4.5 (21)
Behavior Profiling	 4.3 (105)	 4.6 (21)
Data and User Monitoring	 4.5 (104)	 4.8 (21)
Application Monitoring	 4.3 (104)	 4.8 (21)
Analytics	 4.4 (141)	 4.6 (21)
Log Management and Reporting	 4.5 (102)	 4.8 (20)
Deployment/Support Simplicity	 4.4 (103)	 4.6 (21)
Customer Experience		
Evaluation & Contracting	 4.5 (144)	 4.4 (51)
Pricing Flexibility	 3.8 (92)	 3.9 (44)
Integration & Deployment	 4.4 (144)	 4.6 (51)
Ease of Deployment	 4.2 (92)	 4.2 (44)
Service & Support	 4.4 (144)	 4.6 (51)
Timeliness of Vendor Response	 4.2 (93)	 4.5 (43)
Quality of Technical Support	 4.3 (93)	 4.7 (43)

3. Deployment & Target Industry

Splunk: Splunk is primarily developed to be deployed as a software on-premise as a SaaS solution on Splunk cloud. It can also be deployed on public or private cloud and even Hybrid cloud (a combination of private and public cloud)

Splunk is essentially used for industries that are heavily regulated. E.g., Oil and Gas, Financial services, healthcare, Banks, Airline and Railways, nuclear plants, space research organizations, etc.

QRadar: QRadars is available as on-premises hardware or software or in the cloud. Smaller customers can offload all the deployment and maintenance to an IBM cloud-based solution, while larger firms can choose either an on-premises deployment or adopt a hybrid approach collecting data from local and cloud-based applications

QRadar is used in enterprises and moderately regulated industries. E.g., private IT corporations, small to large companies.

4. Fundamental Comparison (Pricing, Metrics, and Intelligence)

We've seen that QRadar is used in Medium to Large organizations, and Splunk is deployed in small-scale enterprises. We'll see some detailed analysis of both these products based on:

- Pricing
- Metrics
- Intelligence

We'll discuss these components for Splunk and QRadar:

1. Splunk:

- **Pricing:** Based on max daily data volume, starting at \$1,800/GB/day.
- **Metric:** Based on the number of users & amount of data ingested per day (Several petabytes/day).
- **Intelligence:** Integrates with Splunk User Behaviour Analysis (UBA) and Machine Learning Toolkit.

2. QRadar:

- **Pricing:** Cloud: \$800/month On premise: \$10,400.
- **Metric:** Based on Events Per Second (EPS) and Flows Per Second (FPS).
- **Intelligence:** Ideal for UBA, IBM Watson, and packet inspection.

5. Pros and Cons of Splunk

After going over the basic comparison between the two, here are some insightful findings:

Pros:

- Easiest to get any sets of data using the rich UI and APIs.
- Splunk Stream can collect network traffic for analysis, and the Splunk Universal Forwarder can be used as a lightweight agent for endpoint analysis.
- This advanced technology has the edge over its competitors by providing real-time data processing, which has been achieved due to the advancement in the processors and hardware of devices.

Cons:

- Splunk is not an open-source technology.
- The overall cost of implementation is initially high.

6. Pros and Cons of IBM QRadar

Pros:

- Excellent fit for the midsize to large enterprises that require SIEM as well as those seeking a unified dashboard for managing a wide range of security monitoring.
- One of its kind sets of functions which help the user to manage their logs efficiently (application, compliance, network overview, risk, system & threat monitoring).

Cons:

- The UBA of Splunk is far superior to the one provided by QRadar. Thus, making QRadar lag in the market.
- Workflow and incident response and management capabilities are better than average, but full potential and automation can be achieved only by opting for IBM's Resilient Incident Response Platform premium solution.

MacAfee ESM and **AlienVault USM** are major competitors of QRadar apart from Splunk.

SOC Analyst Training with InfosecTrain

InfosecTrain has recently introduced its custom-designed SOC Analyst training program to help to aspire and current SOC Analysts. The training program aims at providing the necessary skills to the L1, L2, and L3 SOC Analysts. Check out the course content and the latest schedule of our SOC Analyst training program:

InfosecTrain's [SOC Analyst Expert Training](#)

Get yourself enrolled in our IBM Security QRadar training and get hands-on experience in administering, managing, and tuning the IBM QRadar SIEM solution.

InfosecTrain's [IBM Security QRadar SIEM Training](#)



IND: 1800-843-7890 (Toll Free) / US: +1 657-221-1127 /
UK : +44 7451 208413



sales@infosectrain.com



www.infosectrain.com