Magic Quadrant for Security Information and Event Management

Published: 10 August 2016 **ID:** G00290113
Analyst(s):
Kelly M. Kavanagh, Oliver Rochford, Toby Bussa

Summary

The need for early targeted attack detection and response is driving the expansion of new and existing SIEM deployments. Advanced users seek SIEM with advanced profiling, analytics and response features.

Strategic Planning Assumption

By the end of 2017, at least 60% of major SIEM vendors will incorporate advanced analytics and UEBA functionality into their products.

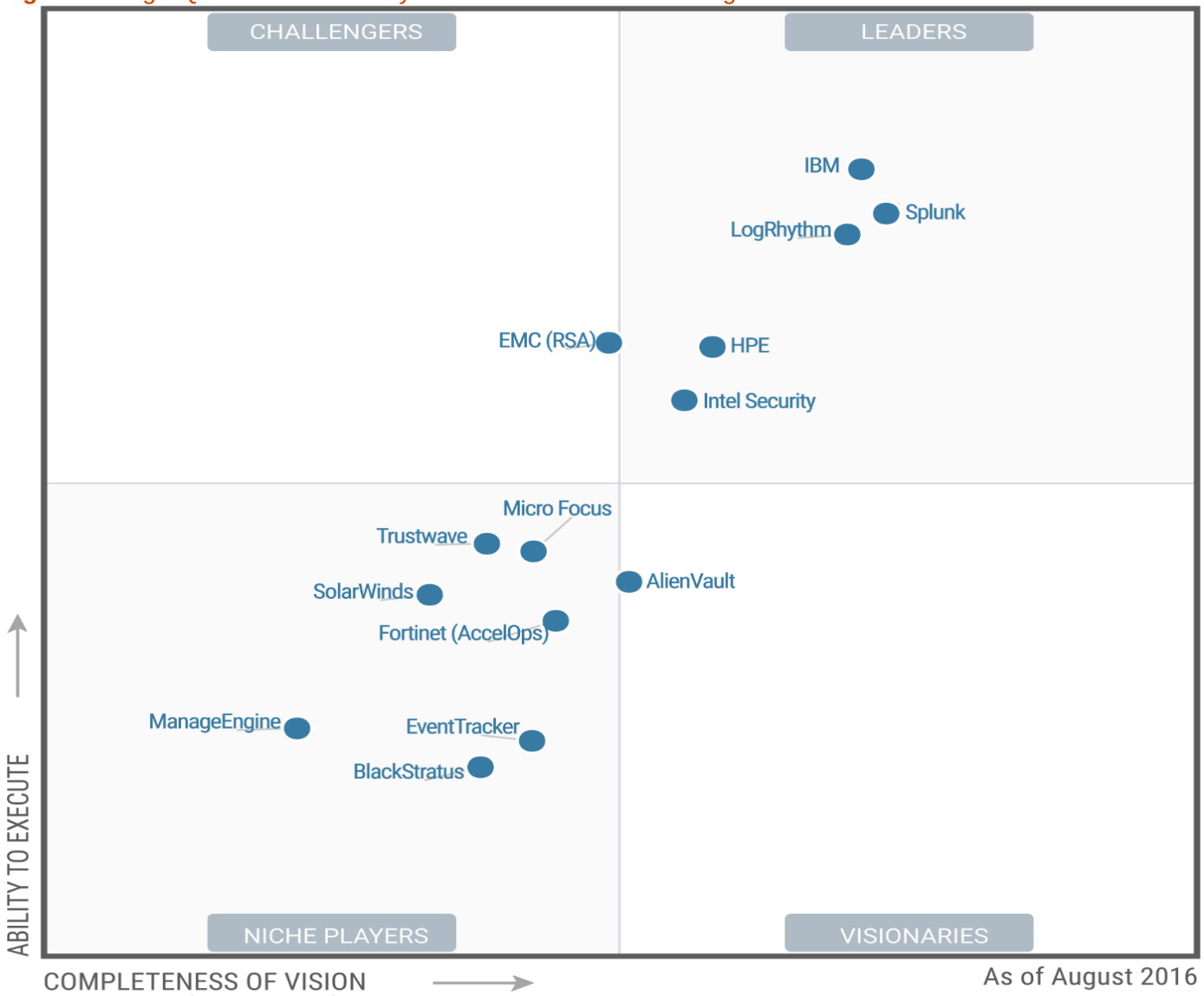
Market Definition/Description

The security information and event management (SIEM) market is defined by the customer's need to analyze event data in real time for the early detection of targeted attacks and data breaches, and to collect, store, investigate and report on log data for incident response, forensics and regulatory compliance. The vendors included in our Magic Quadrant analysis have products designed for this purpose, and they actively market and sell these technologies to the security buying center.

SIEM technology aggregates event data produced by security devices, network infrastructure, systems and applications. The primary data source is log data, but SIEM technology can also process other forms of data, such as NetFlow and network packets. Event data is combined with contextual information about users, assets, threats and vulnerabilities. The data is normalized, so that events, data and contextual information from disparate sources can be correlated and analyzed for specific purposes, such as network security event monitoring, user activity monitoring and compliance reporting. The technology provides real-time correlation of events for security monitoring, query and analytics for historical analysis and other support for incident investigation and compliance reporting.

Magic Quadrant

Figure 1. Magic Quadrant for Security Information and Event Management



Source: Gartner (August 2016)