Gartner Magic Quadrant SIEM Leader rating for Rapid7 IDR

In less than three years, Rapid7 has quickly evolved from its original status as an on-premise vulnerability management company to a leading cloud-based, multi-product security company. This is evidenced by its positioning as a Leader in the Gartner 2020 Magic Quadrant for SIEM (Security Information and Event Management).

“Pre-2015, the normal security tools within organisations were largely negated by attacks occurring within the boundaries of the organisations, with hackers easily circumnavigating the general rules. Rapid7 undertook a mapping process to see how this was happening using a behavioural analytic tool – User Insights. While this platform was really good, we realised that the addition of a log data platform would provide further enhanced benefits for customers,” says Ellis Fincham, director of detection and response for EMEA at Rapid7.

“After acquiring Logentries in 2015, we were able to provide companies with a powerful log tool and fast search function. Together, the Logentries capabilities and Rapid7’s User Insights launched us into the SIEM field. Initially considered as a mainstream offering, the solution soon gained traction in the SIEM sector and led to us being recognised by Gartner as a ‘Visionary’ in the Magic Quadrant for SIEM in 2017. Our extensive investment in research and development has elevated Rapid7 to its current standing in the market,” Fincham adds.

“Further investments in the growth and capabilities of the company have been in our collaborations with synergistic technology providers and in the ongoing development of ‘honeypots’ which lure in hackers and provide us with valuable information on how to proactively counter their attacks based on their breaching methodologies,” Fincham points out.

Rapid7 InsightIDR – engineering better security

InsightIDR — Rapid7’s cloud SIEM — provides a balance of technology and service expertise to enable security leaders to cut through clutter and complexity, while protecting their organisations. The cloud-based software is totally automated and provides quick insights into what is happening within organisations and which tools are required to stop breaches.

Last year Rapid7 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realise by deploying InsightIDR.

“The study, which was undertaken with five existing Rapid7 InsightIDR customers, exhibited some really favourable results, which included an incident management reduction of 38% and a reduction of 27% in false positives. Added to this is the fact that it takes an average of only two weeks to deploy the solution and create a baseline to detect anomalous behaviour in a company, and one month to achieve steady state, with a simultaneous value achievement that is 79% faster than legacy SIEMs,” says Toni Bowker of Cyber Security South Africa (CSSA), distributors of Rapid7 technology solutions in South Africa.

Network Traffic Analysis available to InsightIDR customers

“Network traffic monitoring is an increasingly significant security gap for organisations. Security practitioners looking to minimise their attack surface need to know the types of network data traversing their network and how much of that data is moving: two critical areas that could indicate malicious activity in your environment,” says Bowker.

With its acquisition of leading security analytics and automation provider NetFort last year, Rapid7 is now able to offer its InsightIDR customers Network Traffic Analysis. With deployment of the lightweight Insight Network Sensor, organisations can continuously monitor network traffic at any location or site across their network. This data increases visibility across the attack surface and early detects intrusions (or other potential security events) on the network.

“Attacks generally occur on endpoints and are easy to track. However, with the huge increase in home applications such as smart fridges, this has created an explosion of IPs on customer networks. Manufactured equipment is attached to the network and allows for smarter decision making, but it is essentially on endpoints with no agent, so how do we determine what an attack looks like? With this increase in automation and IoT on stateless assets, hackers will hide in the blind spots and attack the system. Network Traffic Analysis solves this by providing customers with full visibility and allows them to link attacker behaviours together for remedial action,” says Fincham.

“Security teams are stretched to the limit, but by having company security analysts focusing on the low-fidelity attacks and threats on a company’s system, while concurrently deploying InsightIDR to handle the high-fidelity threats, not only can organisations retain the valuable skills inherent in their security team, but they also benefit from total coverage of their systems,” says Fincham.