Exabeam Competitive Solutions Overview

SOLUTION	STRENGTHS	CAUTIONS
exabeam	• Offers phased adoption of a modular solution. • Strong foundation for monitoring users – globally the most deployed UEBA. • Smart Timelines support less-experienced SIEM users by leveraging machine learning, simplifying investigation and response. • Scalable and predictable pricing model based on users. • Extensive portfolio of complimentary technologies (1400+)	• Relatively new to the market and still predominantly purchased in North America. • Often slightly more expensive that competitors due to the complexity of the solution – initially focused at enterprise organisations. • Still building out partner network, especially for services such as managed SIEM.
splunk>	• Multiple delivery options for solution. • Dense ecosystem of partners and technology alliances. • Good reach within organisations, ranging from midsize to large global enterprise.	• Overall scores lower than competitors for evaluation contract negotiation, service, support, pricing and contract flexibility (based on Gartner review) • Lack of endpoint and network sensors means buyers must find additional complimentary solutions. • Own UBA offering not yet integrated with core Splunk. Also only on-premise. • Content only available across individual platforms, all of which licenced separately.
RAPID7	• SAAS option offers quick deployment and initial operation. • Extensive internal portfolio of complimentary technologies. • Strong support for UBA with out the box use cases. • Strong native support for endpoint	• UBA has internal integrations but small technology alliance ecosystem. • Reliance on agents for log collection limits support for IoT and OT use cases. • UBA runs on top of AWS with capabilities subject to licensing conditions of the platform. • Lacking effective application monitoring.
ALIEN VAULT	• SAAS option offers relatively quick deployment and initial operation. • Detection content, rules and dashboards are updated weekly based on findings by Alien Labs Threat Intelligence team. • Strong integrations with other AT&T technologies.	• Integrations with third party solutions is limited. • No native UEBA capability, nor does it integrate with third-party UEBA solutions. • AT&T Cyber received mixed reviews for service, support, log management and real-time monitoring *(based on Gartner customer feedback enquiry)*
IBM QRadar	• Extensive internal resources and partnerships to support sales, deployment and operations. • Open API enabling customers to develop integrations within the platform. • UBA included in base licensing so no additional cost.	• Several licencing models and pricing schemes for various components presents a complex pricing structure. • Customers must deploy third-party products for data-collection from endpoints. • Poor user experience and UI not consistent across entirety of platform. • Increasing reliance on add on products for additional cost to strengthen solution.
LogRhythm The Security Intelligence Company	• Single-vendor-ecosystem with unified solution that includes core capabilities. • Extensive range of professional services. • Extensive range of compliance reports based on product across a variety of industries.	• Outdated SIEM architecture (still a mix of Windows Server, MS SQL & Linux) • Complexity in offering with multiple product names and features – unclear messaging. • Ineffective predefined rules.

Content is directly sourced from Gartner 'Magic Quadrant for Security Information and Event Management' - *Click here to learn more*

For further help please contact: Exclusive Networks team - Exabeam_UK@exclusive-networks.com Harry Brewer, Exabeam Product Sales Specialist - HBrewer@exclusive-networks.com