RIVERSAFE

INTEGRITY, INNOVATION, IMPACT

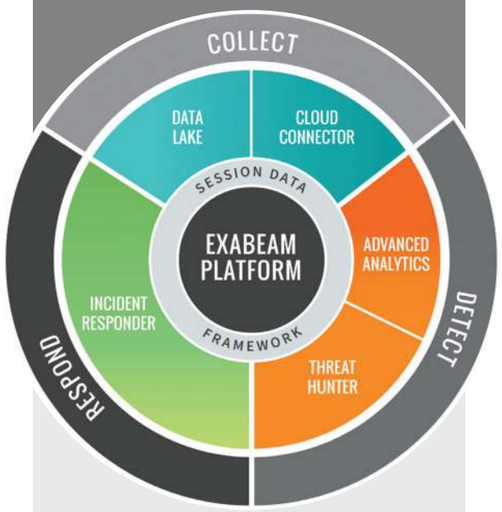
Exabeam Offering

BUSINESS **SOLUTIONS** SHEET

Many organisations use their chosen SIEM to gather compliance logs and some of these are dependent on logging limits, which block the visibility of the complete logs from all the internal systems. Find out how Exabeam and RiverSafe can help you gain unlimited logging capability…

WHY RIVERSAFE?

As an EMEA Exabeam services partner, our professional services consultants pride themselves on providing expert advice in architecture, data quality, ongoing maintenance, and support of Exabeam and its premium apps. Our team consists of qualified consultants who guide our clients through the entire delivery journey, from requirements and planning to design, implementation, adoption and support.



UEBA, THREAT DETECTION AND RESPONSE

Exabeam Data Lake (DL) offers unlimited logging capability to collate the information required and provide more insights into User and Entity Behaviour and Internal Threat Detection though its powerful Machine Learning capability and built in Advanced Analytics (AA). Identified threats can be captured through Case Management and Incident Response (SOAR – Security Orchestration and Automated Response).

UNDERSTAND THE REQUIREMENTS AND GOALS OF YOUR EXABEAM DEPLOYMENT

When we are engaged to implement Exabeam products, RiverSafe plans and prepares for all aspects of the solution to ensure all details that impact success are clearly identified and addressed. From use cases to data sources and data quality, from platform specifications to parsing, primary users and usage - a lack of planning in any one of these factors can jeopardise the delivery. To protect the investment in security programmes it is crucial to have the right technical consulting expertise available and this is what we deliver for our clients.

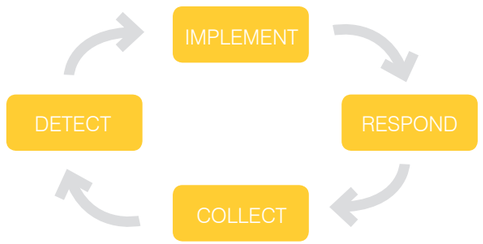
OUR IMPLEMENTATION SERVICES INCLUDE:

Implement:
- Planning and preparation work
- Set up hardware/Set up instances in Cloud
- Validate customer architecture
- Validate customer requirements
- Identify the Exabeam product for implementation
- Implement the Exabeam product
- Install licenses for the products

Collect:
- Set up and configure the Advanced Analytics
- Ingest data into Data Lake
- Ingest data from SIEM
- Validate data sources
- Parser validation

Detect:
- Build the models for threat detections
- Identify the threats
- Set threat hunter

Respond:
- Set up and configure case management
- Set up and configure Incident Responder
- SOAR integration and Playbook configuration
- Test incident generation



PREMIUM OR STANDARD?

The matrix below lists the services covered by our Premium and Standard Offering:
Both offerings start with a 1-week planning and preparation phase. The Standard offering provides an implementation phase of 2 weeks for each of the AA, DL, and IR products. The Premium offering provides an implementation phase of 3 weeks for each of the AA, DL and IR products. Additional professional services days will need to be scoped for IR custom playbooks based on those custom scenarios

	PREMIUM	STANDARD
Planning and prep work	✓	✓
Set up hardware/implement AWS solution	✓	✓
Advanced Analytics	✓	✓
Validate customer architecture	✓	✓
Validate requirements	✓	
Validate use cases	✓	✓
Install software and licenses	✓	✓
AA Set up and configuration	✓	✓
Identify and configure AA and validation (Windows, VPN, 1 security feed, 2 additional feeds)	✓	✓
AA Parser validation (OOTB)	✓	✓
Log source count	Up to 20	Up to 10
AA deployment validation	✓	✓
Threat hunter validation	✓	✓
Advanced Analytics additional Parser creation	✓	
Entity Analytics set up and configuration	✓	
Data Lake		
Data Lake set up and configuration	✓	
DL Parser validation (OOTB)	✓	✓
Incident Responder	✓	
Incident responder set up and configuration	✓	
Create Playbooks	✓	
Case management set up and configuration	✓	
Validate incident creation	✓	
Custom rules (based on OOTB Models)	Up to 10	Up to 5
Custom IR Playbooks**		
Custom data source onboarding and parsers **		

DEPLOYMENT SERVICE	PREMIUM	STANDARD
Planning and prep work	1 Week	1 Week
Advanced Analytics	3 Weeks	2 Weeks
Data Lake	3 Weeks	2 Weeks
Incident Responder	3 Weeks	2 Weeks

PACKAGE NAME	DETAILS
Standard	Starting from £18,000 - £42,000
Premium	Starting from £24,000 - £60,000
This is based on at least one product (AA, DL, or IR) being purchased with a week of prep and planning for either tier	

** Requires additional scoping for PS days

ABOUT RIVERSAFE

RiverSafe provides Cyber Security, Cloud and Analytics services to ensure customers can see and respond to the security threats across their digital enterprise. We enjoy strong partnerships with many market leading vendors enabling us to provide high-value customer solutions. RiverSafe drives innovation for our customers which has enabled us to sustain our continued growth. We have a strong track record of delivering results – largely down to our team of highly experienced consultants with a reputation for delighting customers.
For more information please visit:
www.riversafe.co.uk

WHY RIVERSAFE

We offer a comprehensive capability to enable our customers to accelerate time to value, de-risk deployment and manage business risks.

- Passionate about customer success
- Flexible, highly skilled resources
- Comprehensive suite of services
- Collaborative
- Proven track record
- Vendor endorsed

We offer a comprehensive capability to enable our customers to accelerate time to value, de-risk deployment and manage business risks.

RIVERSAFE
INTEGRITY, INNOVATION, IMPACT

GET IN TOUCH

If you would like to find out more about how RiverSafe can help you please contact us on

Unit 2,
New Concordia Wharf,
Mill Street,
London,
SE1 2BB

+44 (0) 203 633 2577
sales@riversafe.co.uk
www.riversafe.co.uk