You have to take data privacy seriously
Unfortunately your big data environment makes this difficult

Cyber-Threats are serious. It's no longer a matter of if your organization will have to thwart off a cyber-attack, it's when it will happen. Like most organizations, the big data environment has become a critical part of the arsenal to analyze information, and the weakest link in security is normally the big data environment.

Because of recent cyber-threats, governments have begun passing legislation to force organizations to take protecting the privacy information they have been entrusted with seriously. The first legislations are GDPR, planned to go live in May, 2018 with similar legislations expected elsewhere.

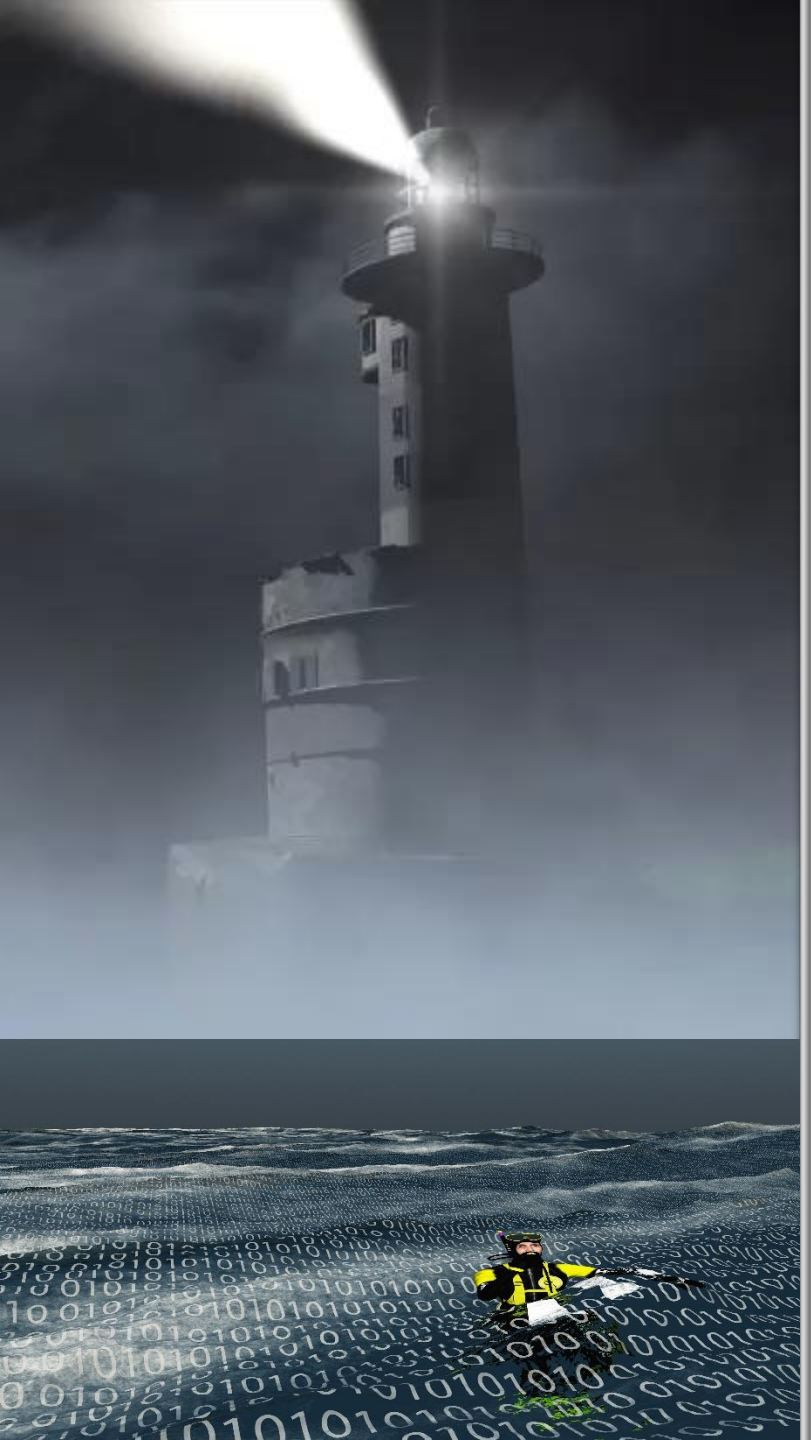
Fortunately, we have a solution to protect Privacy information that finds its way to your big data environment. Please read on for some details about our approach.

BigDataRevealed

Secure/Sequester and Encrypt

By Steven Meister 847-791-7838 EUGDPRWebinars@bigdatarevealed.com

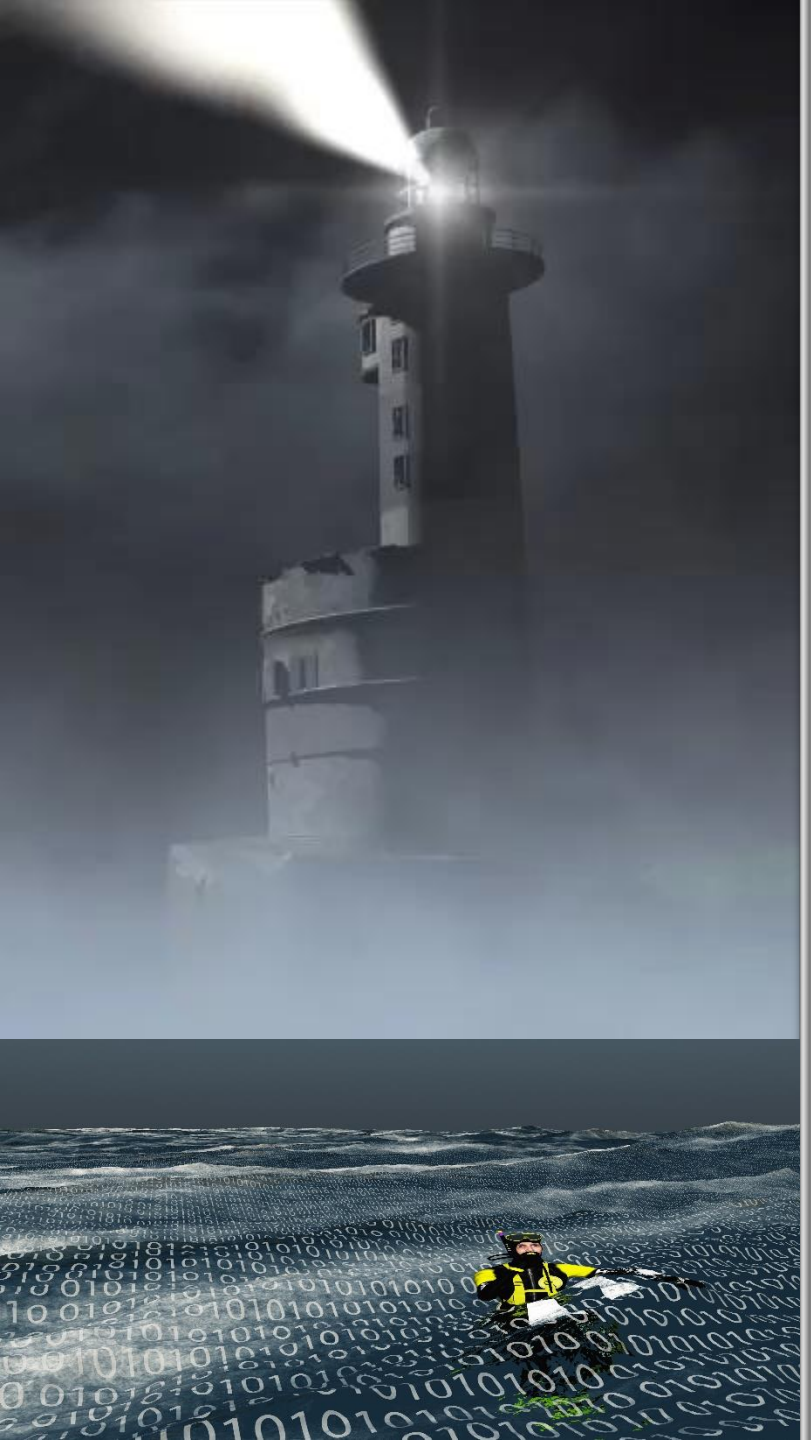
Big Data Revealed
RADAR FOR YOUR DATA LAKE



BigDataRevealed uses the Intelligent Catalog

Our first product was the intelligent catalog, which is the base from which the Secure/Sequester and Encrypt (SSE) process we use to protect information in your big data environment is derived.

The Intelligent Catalog is the missing directory for Big Data that also has analytic capabilities. We use these analytic capabilities to identify patterns in registered files and streaming data to protect privacy information entrusted to you that should not be unprotected in your big data environment.



How it works

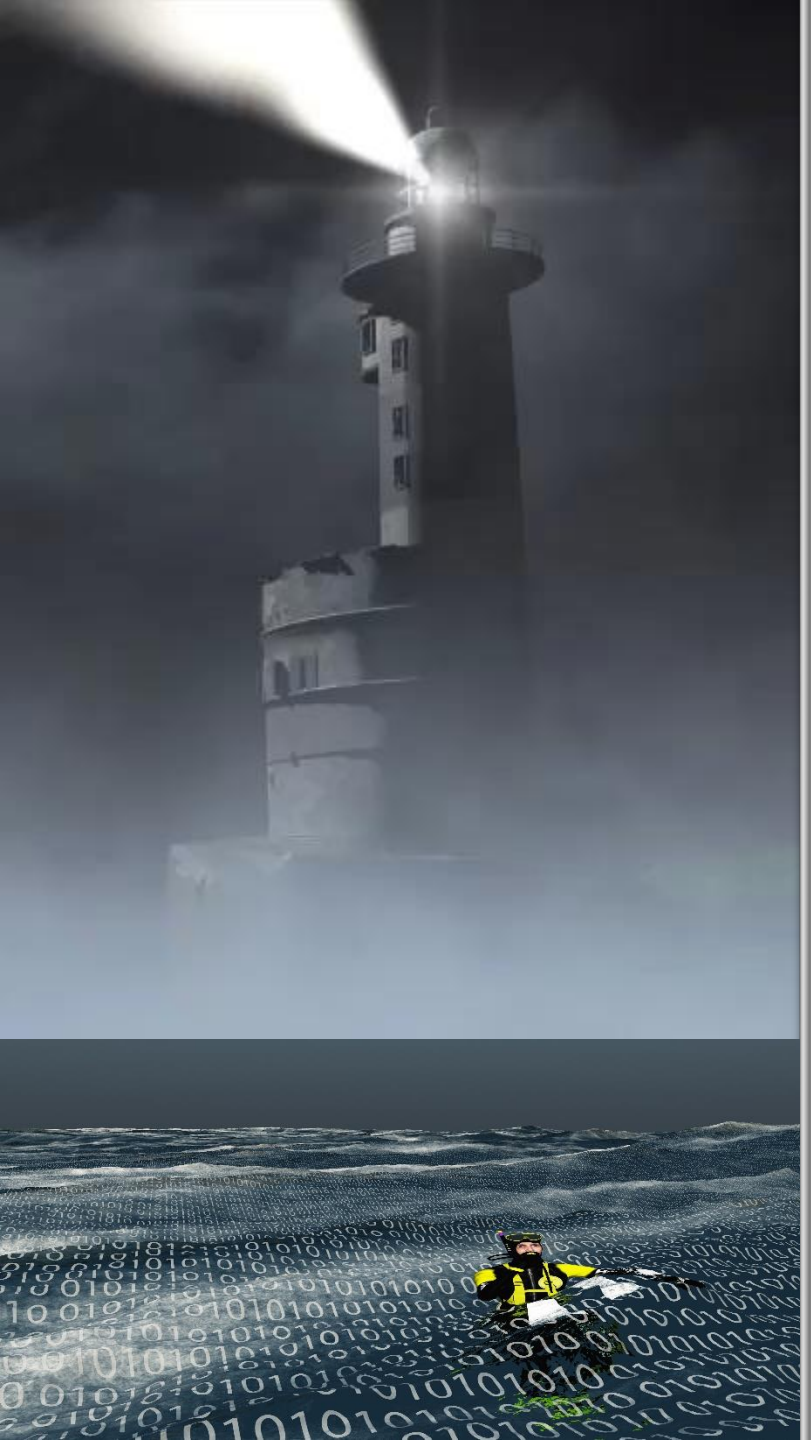
Data files and streams are registered to the SSE facility

- This registration process defines what to protect
- Patterns that are not privacy information are registered as false positives (i.e., vendor numbers, invoice numbers, etc. that have similar patterns to social security or credit card numbers).

When files and streams are presented to the big data environment, the intelligent catalog goes to work

- It stores the identity of the file or stream and stores metadata about the file or stream
- It uses the rules written about the patterns and determines if the patterns are on the false positive list
- Real patterns are passed to the SSE facility for corrective action

The SSE engine goes to work to sequester privacy information, encrypt the privacy information in the big data environment and secure the encryption keys into a protected area.



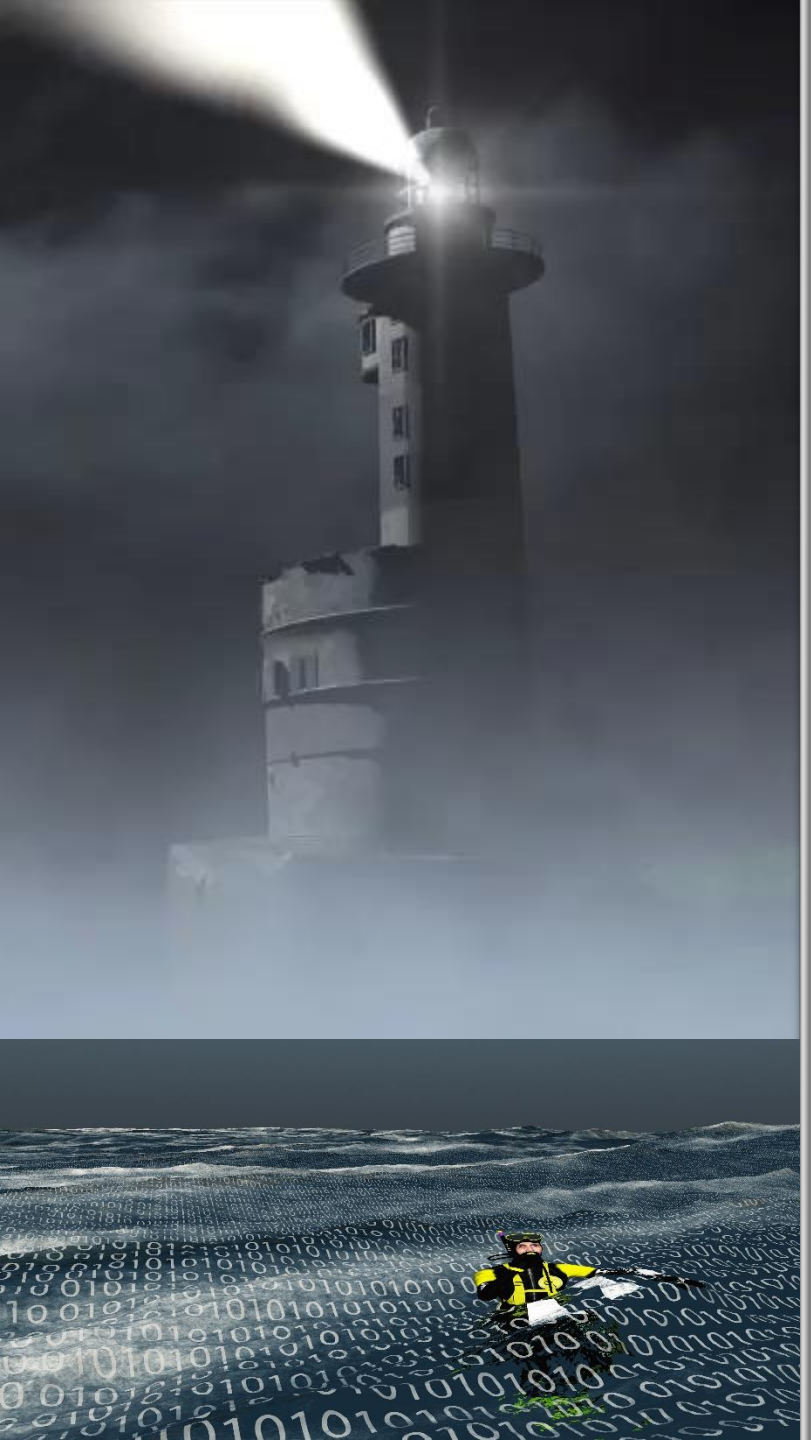
Use the intelligent catalog to identify potential PII issues in incoming streams

1. As BigDataRevealed does for static data at rest in HDFS and Hbase, BDR uses its same BDR-Libraries and engine to discover patterns of sensitive data and applies its SecureSequester/Encryption methods to incoming streams of data and encrypts the PII before it ever gets written into your Data Lake.

2. The producer is the management workbench used to configure the streams that should be interrogated by BigDataRevealed's SecureSequester

3. The patterns in the streams are identified and false positives are eliminated, leaving what is potentially exposed Personal Identifiable Information (PII)

4. The SecureSequester capabilities of BigDataRevealed's Intelligent Catalog then go to work to encrypt PII data and sequester the keys necessary to reveal PII values

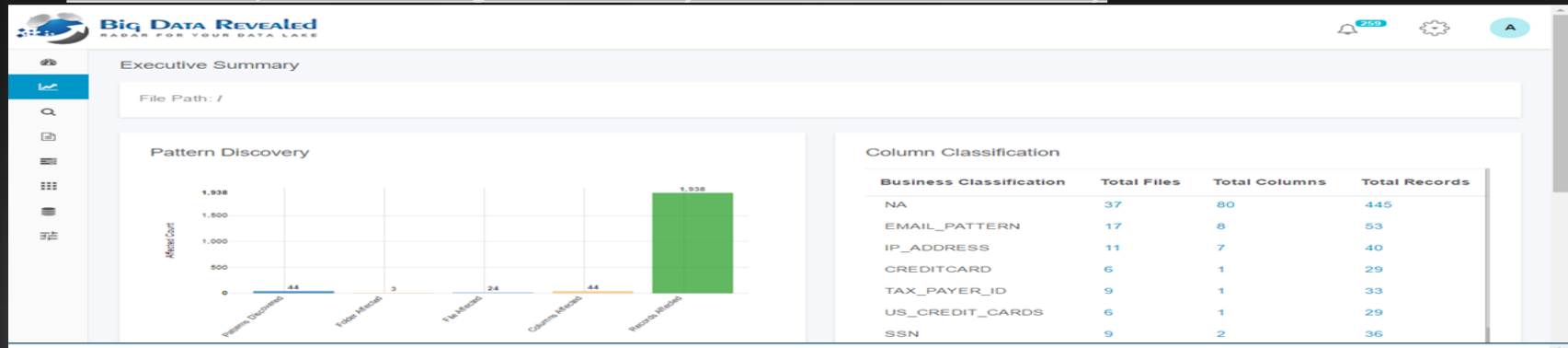


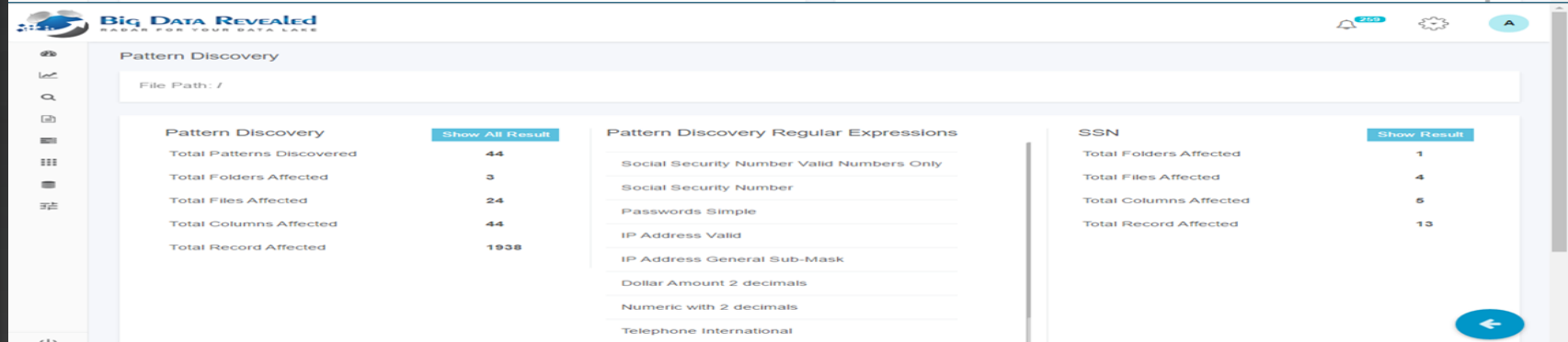
How the potential issues are reviewed

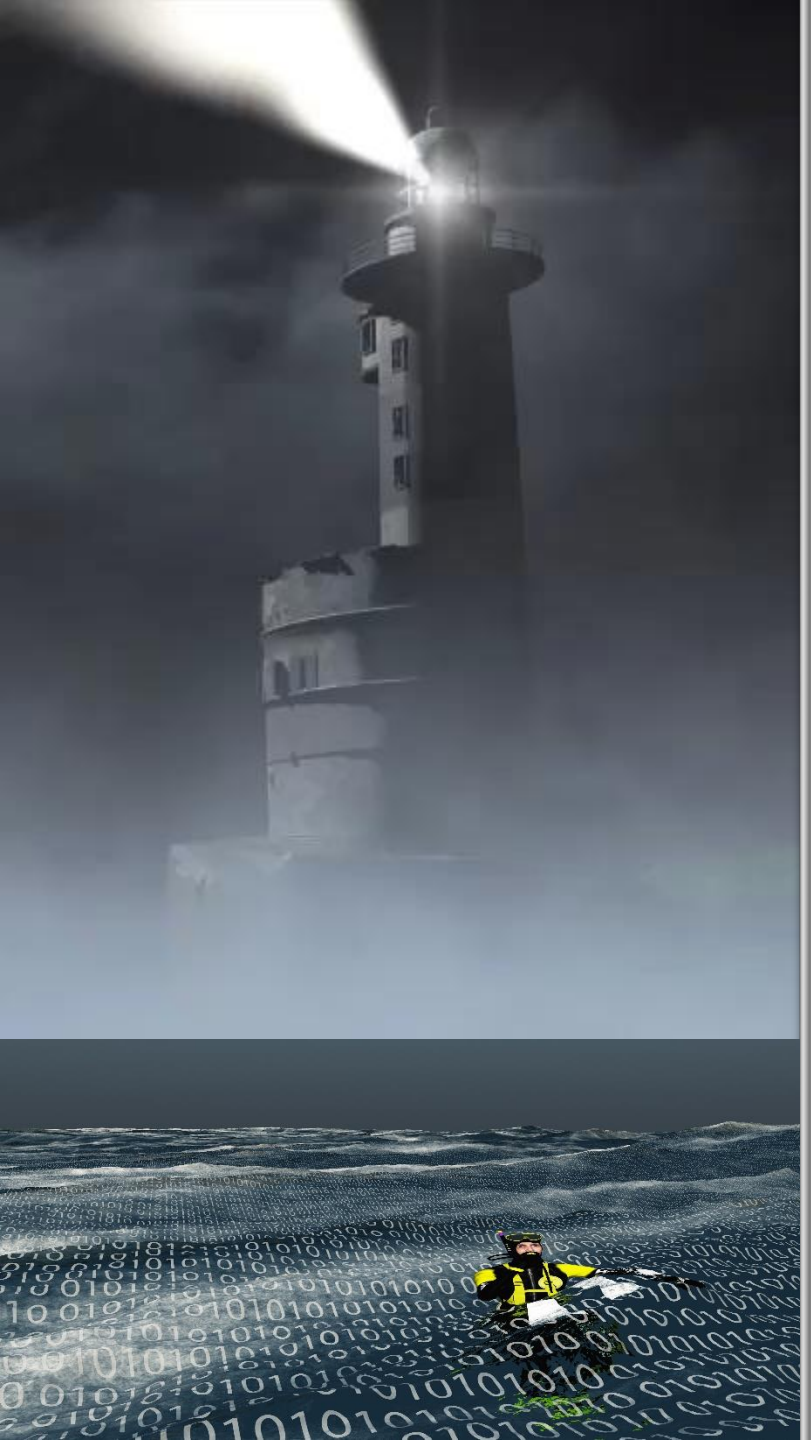
- ✓ BigDataRevealed and its Intelligent Catalog are available in its Executive Summary as well as its Data Scientist Toolkits Graphical Interface. The Intelligent Catalog can also be accessed by most any other third party tools.
- ✓ Users can view PII by type of Business Classification such as email, names, addresses, SSN, Banking Information, Credit Cards and a limitless amount of PII Discoveries.
- ✓ With the Use of Drilling, Users can see the high-level summary counts of PII by category as well as drill down to a single system source of record for a PII exposure.
- ✓ The BDR Intelligent Catalog is collaborative and available to other Metadata tools/repositories and can be exported as well as can import Catalog and metadata.

How someone with appropriate clearance would use encrypted data:

- ✓ ***Collaborative, sharable though controlled by Users Roles Based Authority***







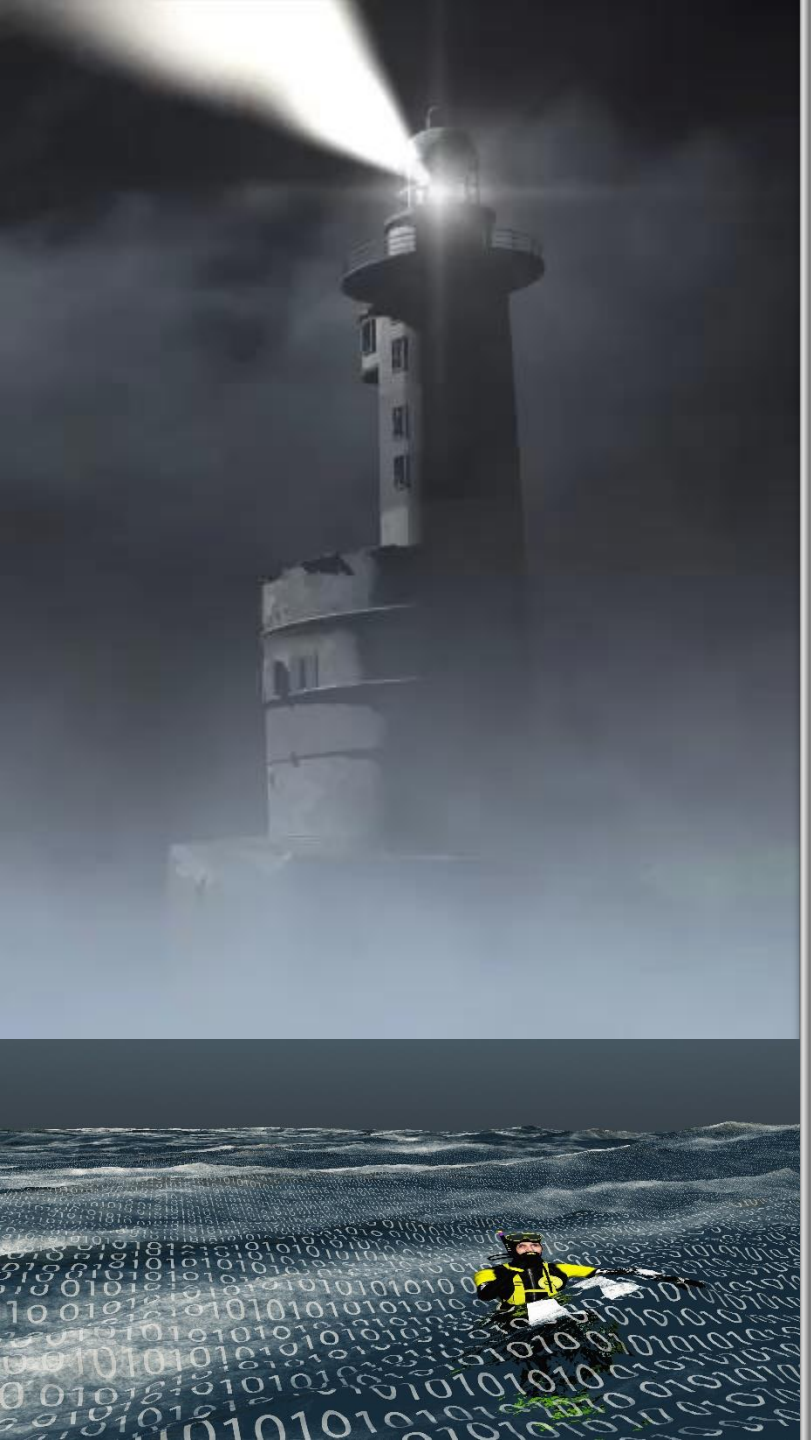
In Summary BigDataRevealed Steps

BigDataRevealed Discovery

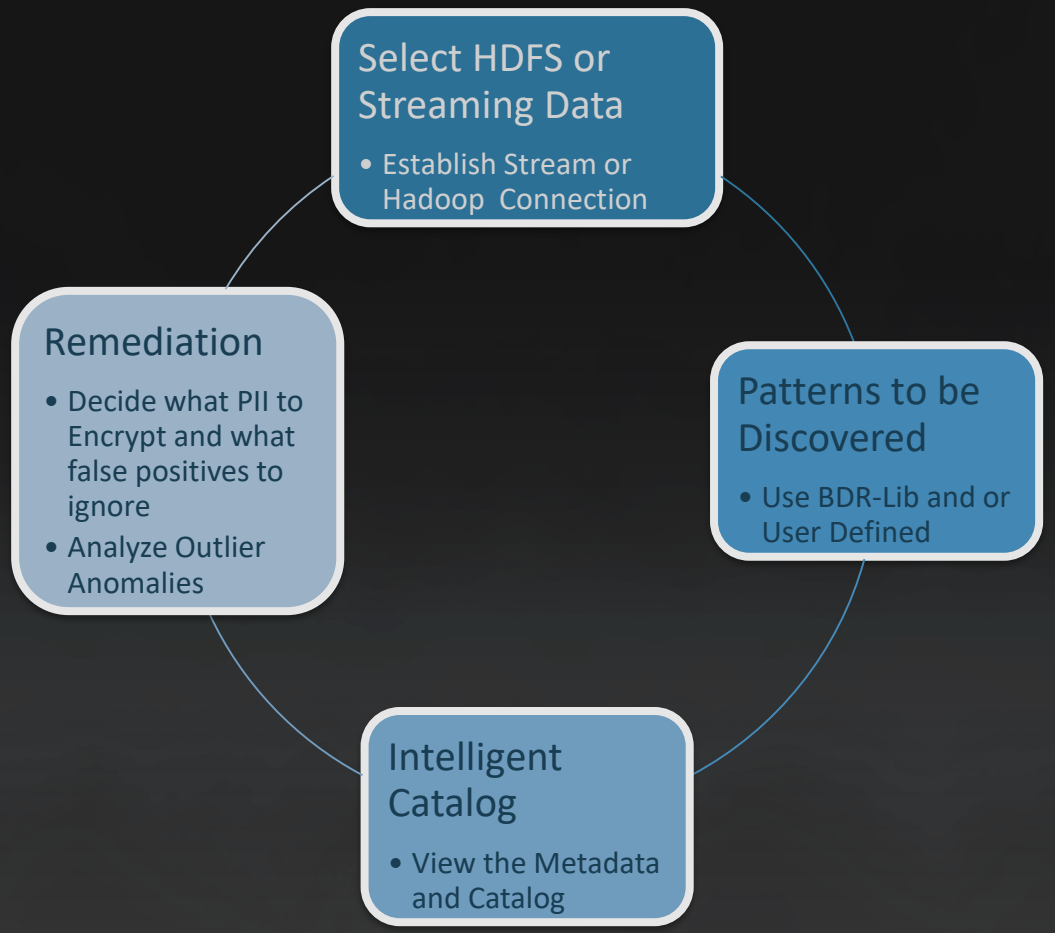
BigDataRevealed Intelligence Catalog & Metadata

BigDataRevealed SecureSequester & Encrypt

BigDataRevealed Validate Remediation



BigDataRevealed Repeatable, Collaborative Application Process



BigDataRevealed Executive Summary screen and the SecureSequester/Encryption Interface