IBM Security

IBM Security Guardium Analyzer Bootcamp

IBM SECURITY

Larry Lindsay, Devan Shah

October 2018

IBM

Overview

Agenda

- Why Does Data Compliance Matter?
- Introduction to IBM Security Guardium Analyzer
- How Analyzer works?
- How Analyzer performs risk assessment?
- Hands-on Workshop To setup IBM Security Guardium Analyzer

Data Compliance

Data Compliance: GDPR

WHAT'S NEW?

THE DEFINITION OF WHAT CONSTITUTES 'PERSONAL DATA' NOW INCLUDES MUCH MORE, SUCH AS...

- EMAIL ADDRESS
- COOKIE STRINGS
- LOCATION
- IP ADDRESS
- GENETIC DATA
- BIOMETRIC DATA
- HEALTH DATA

PENALTIES
FOR NON-COMPLIANCE INCLUDE FINES OF UP TO

€20 MILLION

OR 4% OF GLOBAL TURNOVER

WIDER GEOGRAPHICAL SCOPE

GDPR applies to all companies processing the personal data of people who live in the EU

CONSENT

Consent must be freely given, specific, informed and unambiguous – with a positive opt in

AND YOU MUST BE ABLE TO PROVE IT!

NEW RIGHTS OF THE DATA SUBJECT

- the right to be informed
- the right of access
- the right to rectification
- the right to restrict processing
- the right to data portability
- the right to object
- the right not to be subject to automated decision-making

Introducing … IBM Security Guardium Analyzer

Start fast

This software-as-a-service offering helps you get started immediately with a guided setup process.

Protect data

Specifically designed to help identify regulator data risks, this service analyzes on-premises and cloud databases to find and present users with prioritized risk information.

Next-generation data classification

A next-generation classification engine, which also powers IBM Watson offerings, searches data inside cloud and on-premises database tables, and vulnerability scanning uncovers current threats.

Reduce time to value

Pre-built functionality and dynamic dashboards surface data exposures, providing information such as: number of databases affected, severity breakdown, geographic breakdown.

Take action to minimize risk

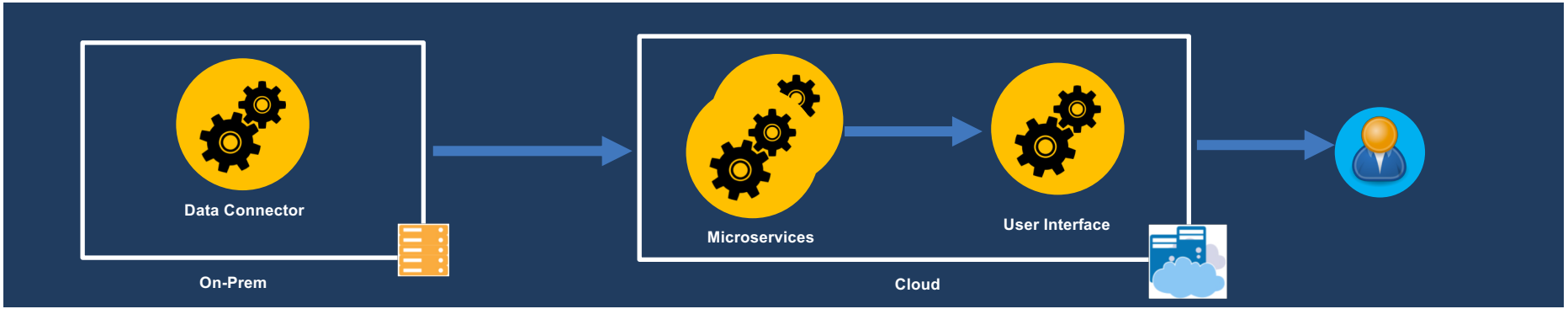
This service combines the data classification and vulnerability scanning results to provide risk scoring and prioritization information so you can efficiently take focused steps to minimize risk.

Streamline regulator activities

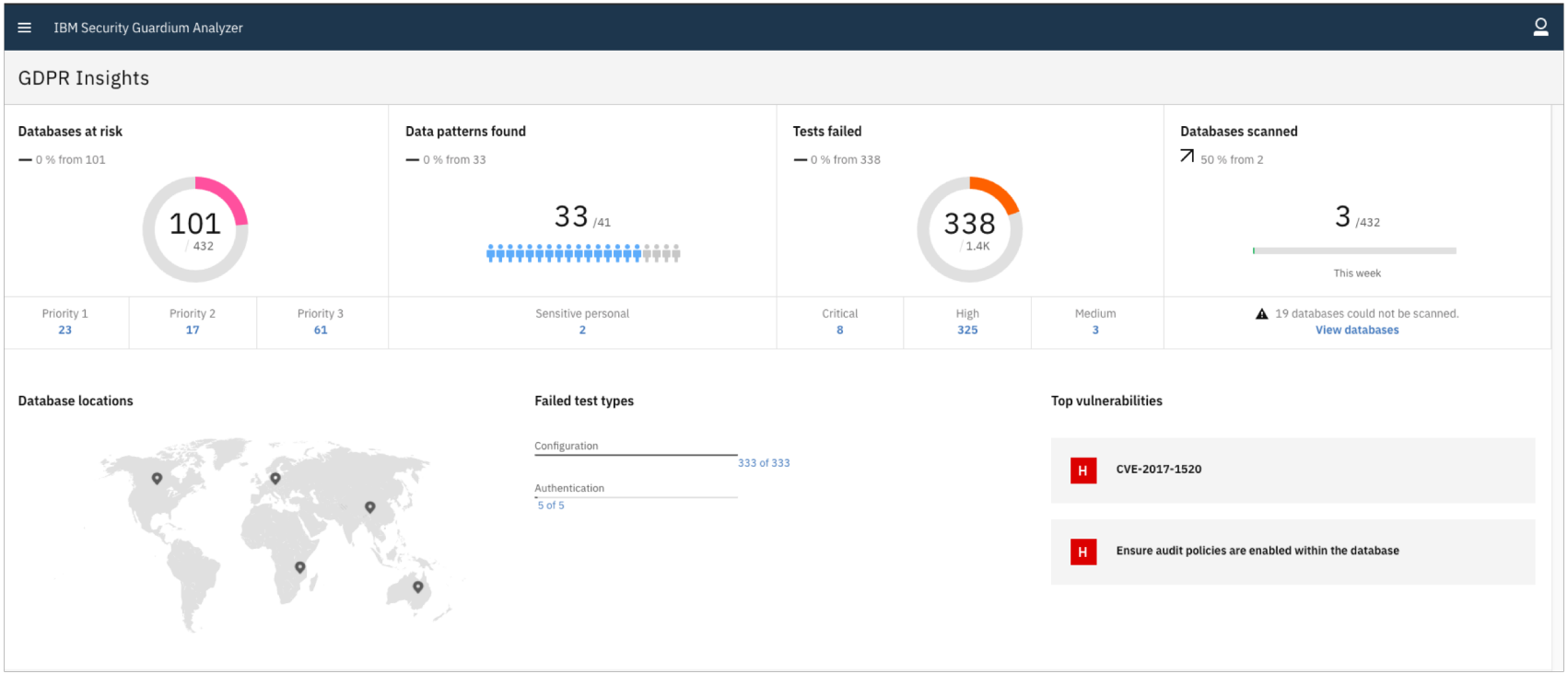
Helps compliance managers, data managers and IT managers get the information they need, at the right level of detail, to collaborate efficiently.

How it works?

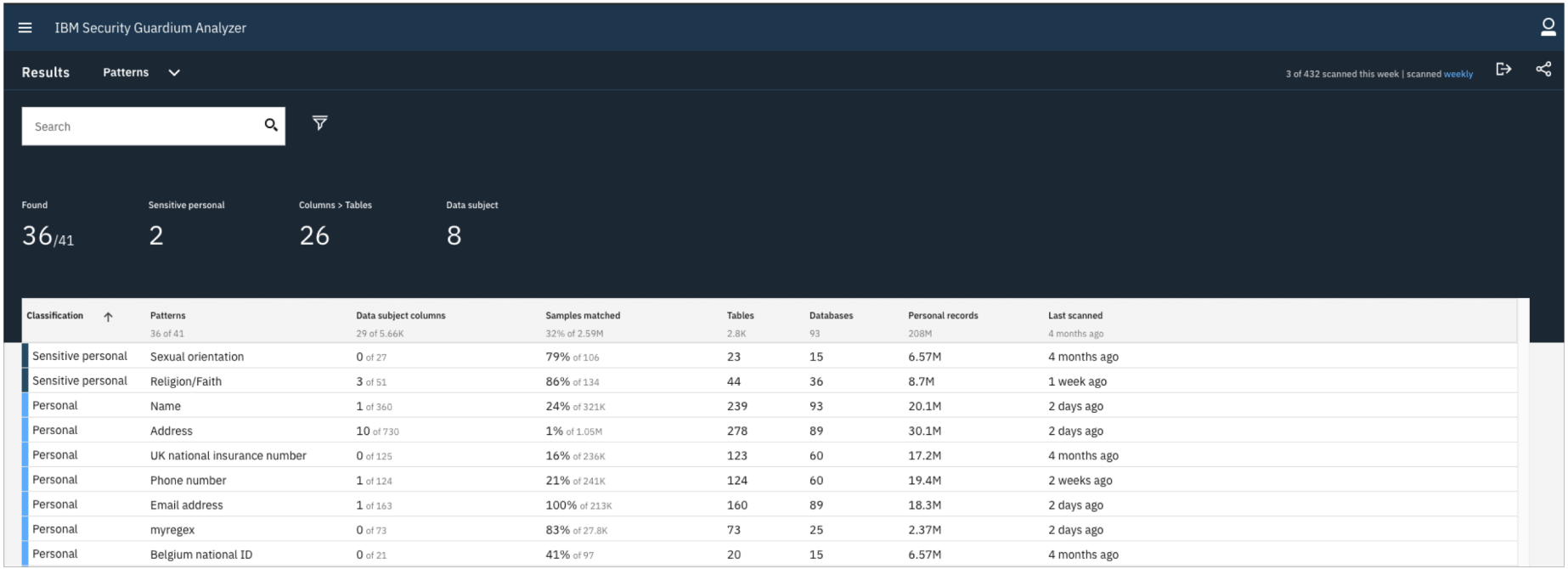
- On-Prem Data Connector
  - Classification Scans
  - Vulnerability Scans
- Cloud Microservices
  - Parsers
  - Risk Engine
  - Classification Rules Management
  - Data Aggregators
- Data Visualizations
  - Provide all the data to the users



Overview: Global Dashboard

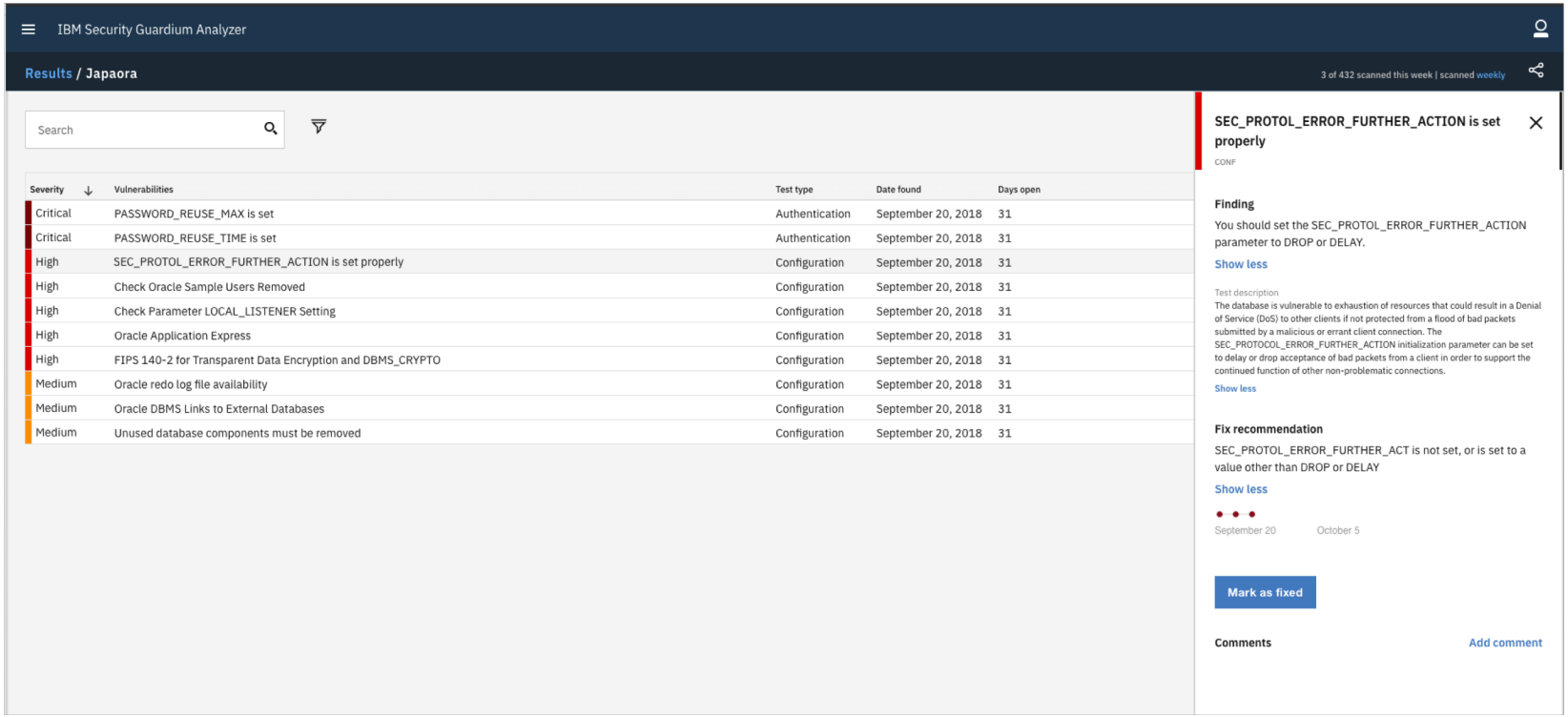


Overview: Regulator Data Insights



Classification	Patterns (36 of 41)	Data subject columns (29 of 5.66K)	Samples matched (32% of 2.59M)	Tables (2.8K)	Databases (93)	Personal records (208M)	Last scanned (4 months ago)
Sensitive personal	Sexual orientation	0 of 27	79% of 106	23	15	6.57M	4 months ago
Sensitive personal	Religion/Faith	3 of 51	86% of 134	44	36	8.7M	1 week ago
Personal	Name	1 of 360	24% of 321K	239	93	20.1M	2 days ago
Personal	Address	10 of 730	1% of 1.05M	278	89	30.1M	2 days ago
Personal	UK national insurance number	0 of 125	16% of 236K	123	60	17.2M	4 months ago
Personal	Phone number	1 of 124	21% of 241K	124	60	19.4M	2 weeks ago
Personal	Email address	1 of 163	100% of 213K	160	89	18.3M	2 days ago
Personal	myregex	0 of 73	83% of 27.8K	73	25	2.37M	2 days ago
Personal	Belgium national ID	0 of 21	41% of 97	20	15	6.57M	4 months ago

Overview: Vulnerability Assessment

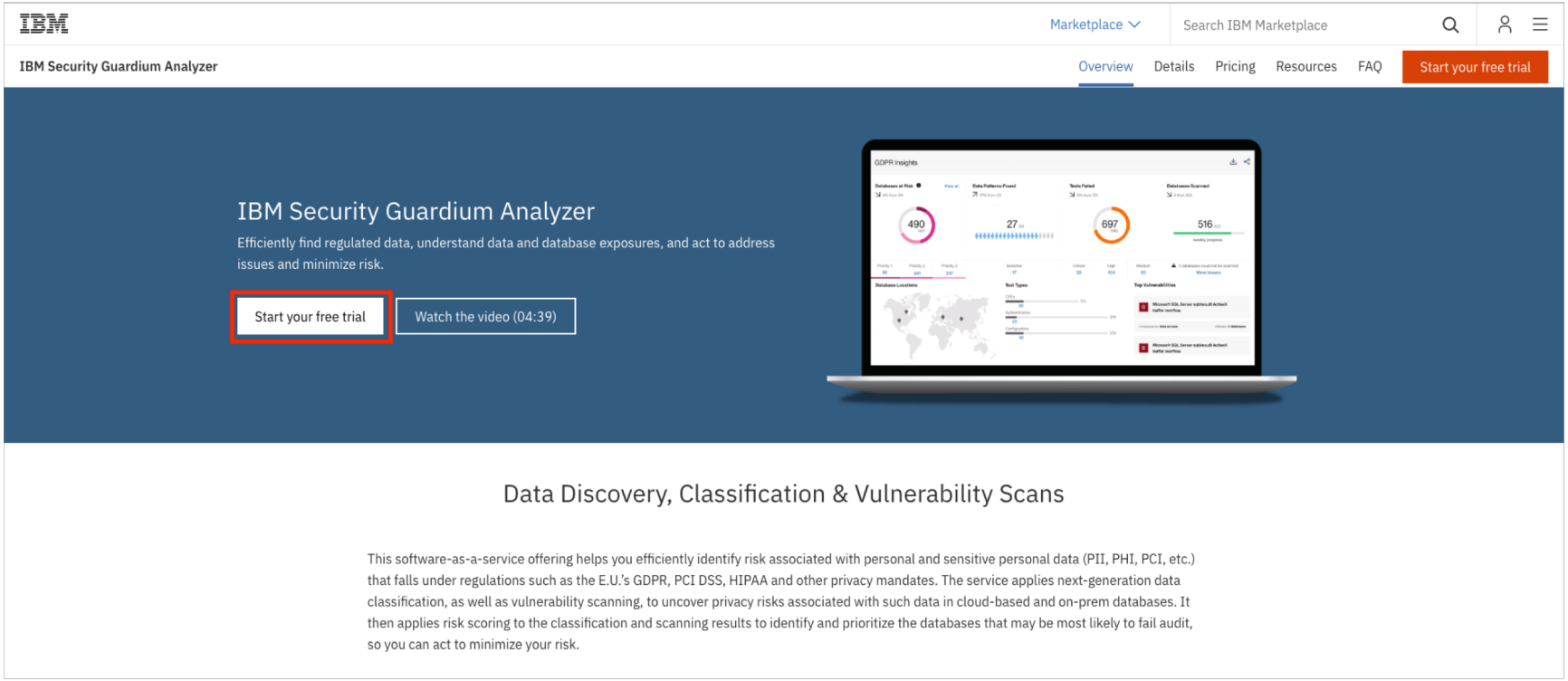


Database Risk

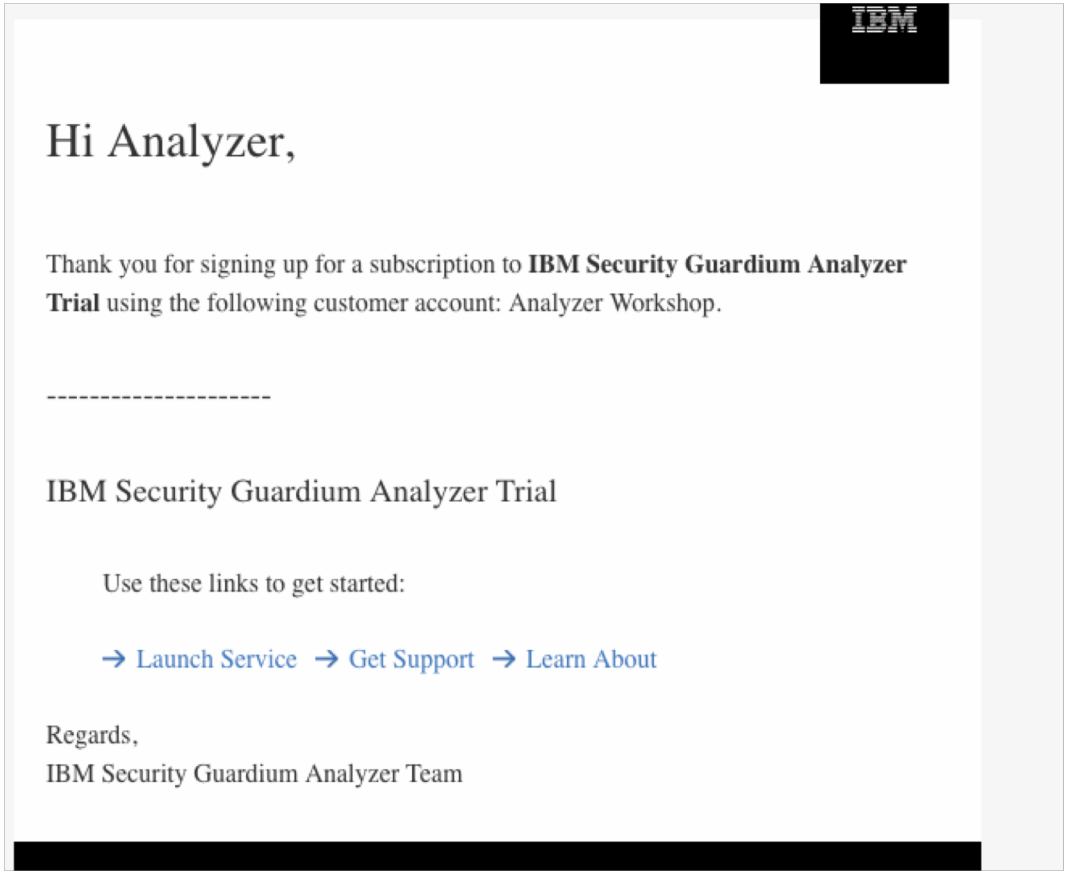
- Exposed Regulator Data
  - Sensitive Personal Information, or SPI
    - Also called ”special category” data
  - Personally Identifiable Information, or PII
- Vulnerabilities
  - CVEs
  - Default Database Settings
  - Permissions

Workshop: Free Trial

Workshop: Marketplace



Workshop: Ready Email



IBM

Hi Analyzer,

Thank you for signing up for a subscription to **IBM Security Guardium Analyzer Trial** using the following customer account: Analyzer Workshop.

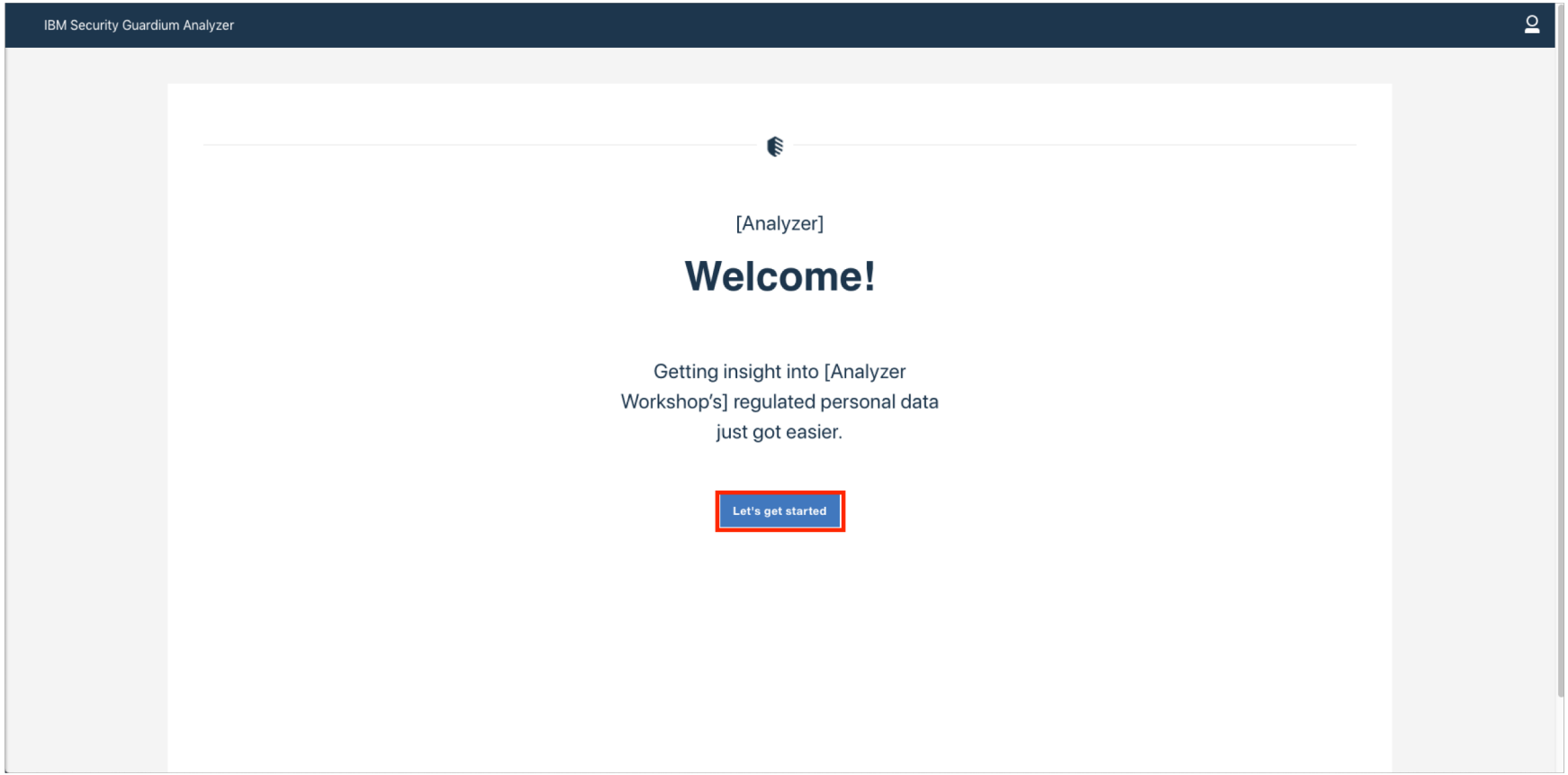
IBM Security Guardium Analyzer Trial

Use these links to get started:

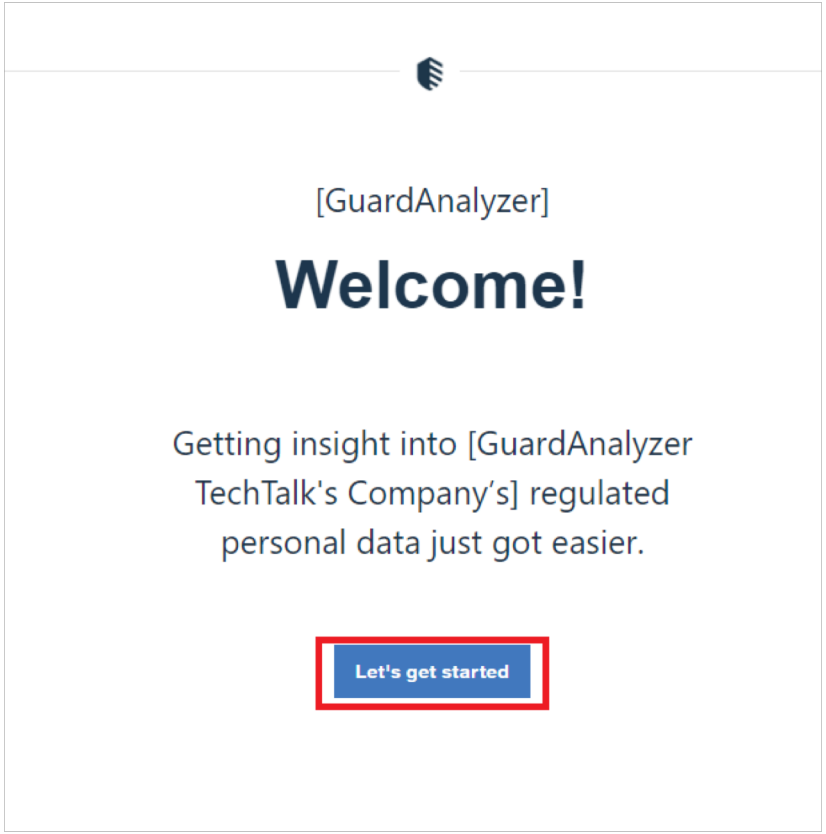
→ Launch Service → Get Support → Learn About

Regards,
IBM Security Guardium Analyzer Team

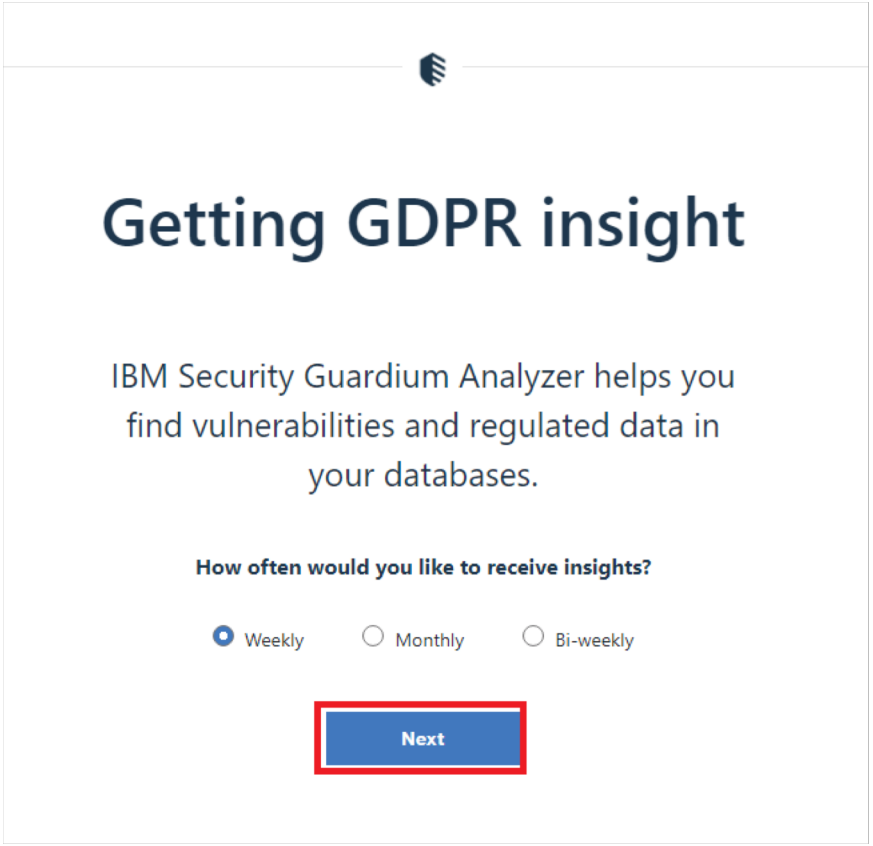
Workshop: Analyzer Welcome Page



Workshop: Getting Started

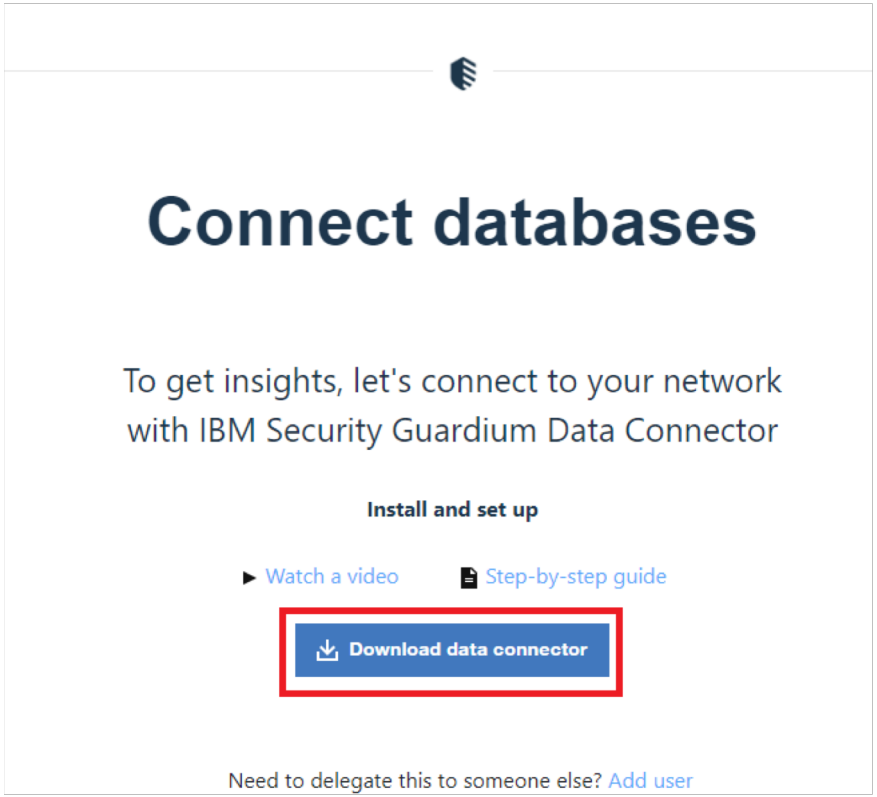


Workshop: Insight Settings



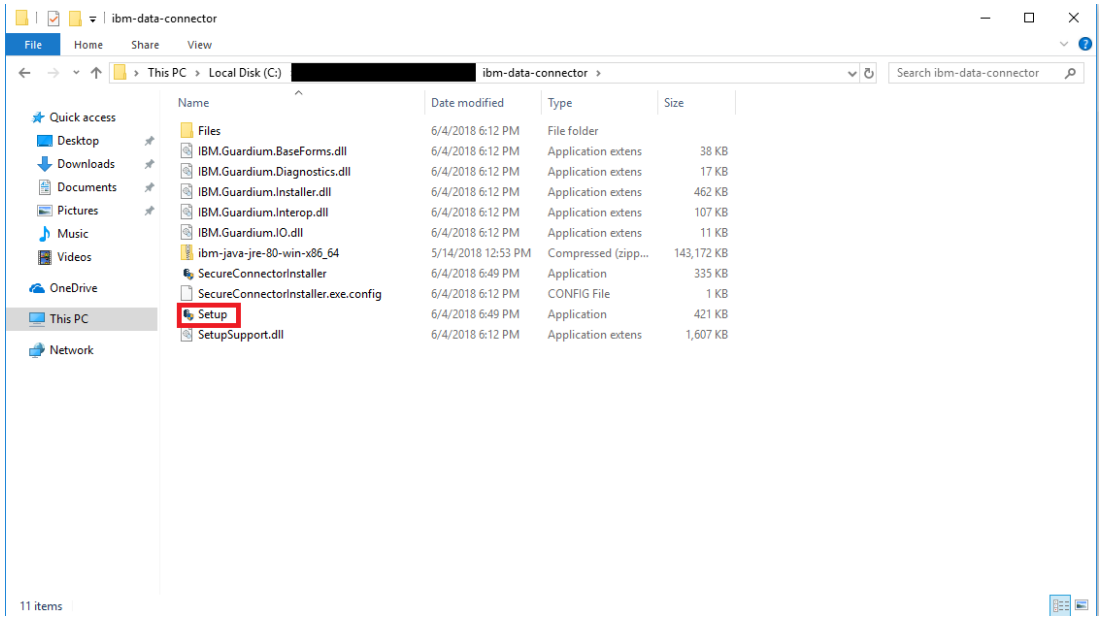
- **Select how frequently Analyzer will scan your databases**

Workshop: Download Data Connector



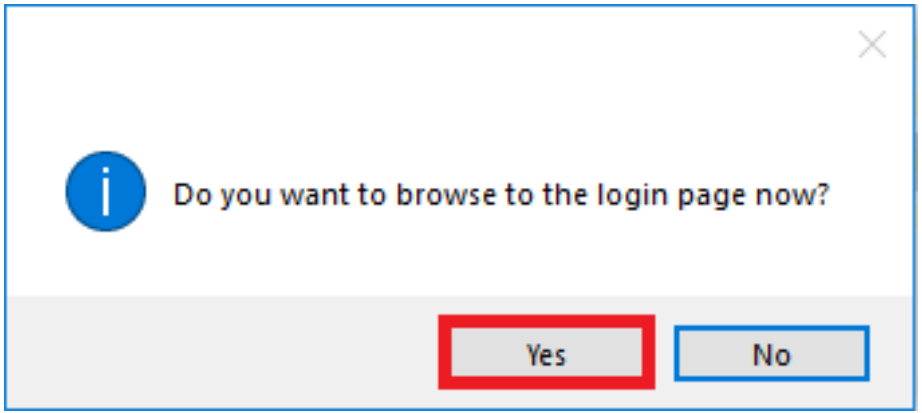
- **Video and Guide to walkthrough setting up Data Connector**
- **Download Button to get latest Data Connector Package**

Workshop: Run Setup



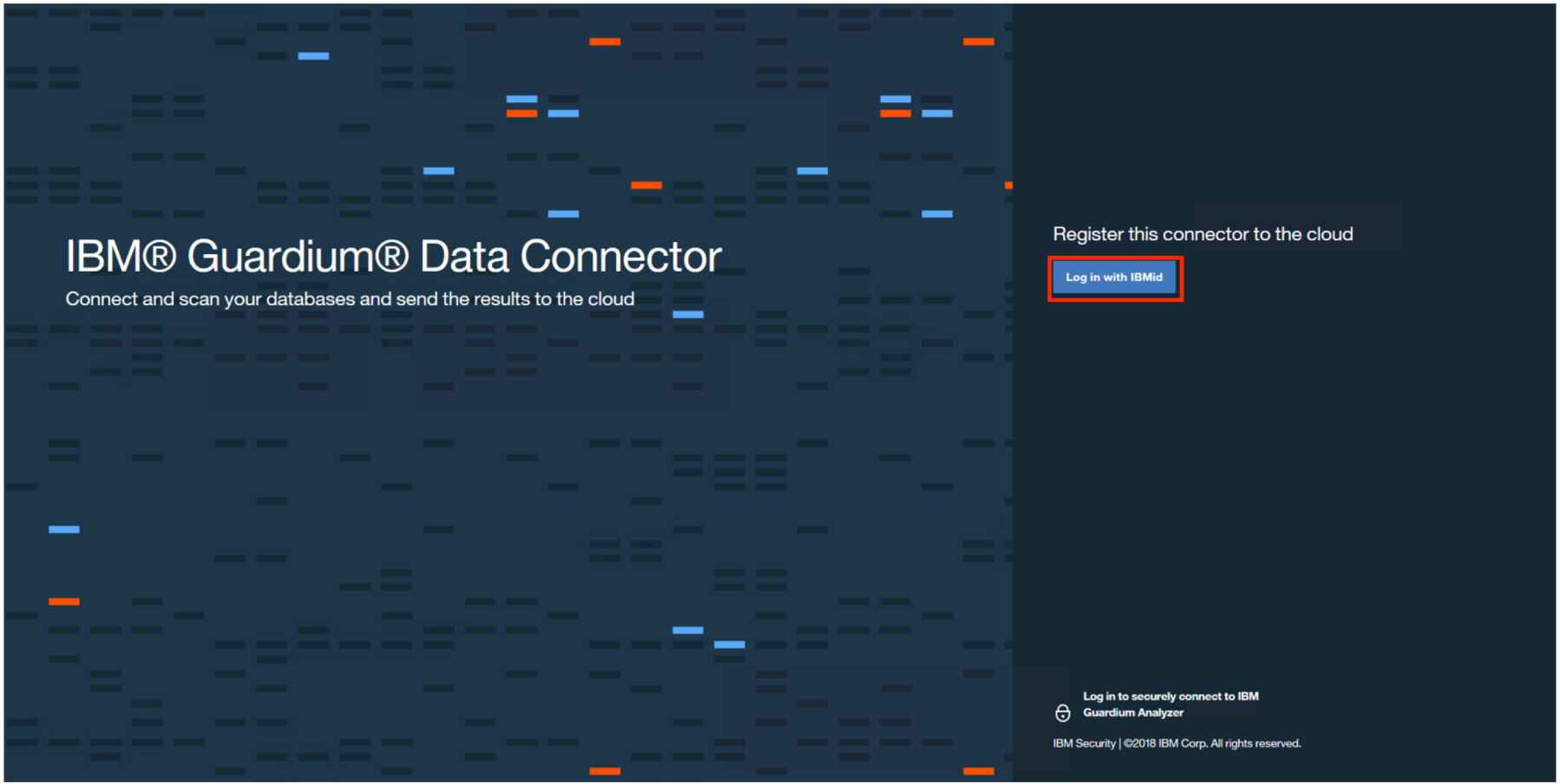
- Unzip Data Connector package that was downloaded
- Run Setup.exe and run through installer

Workshop: Navigate to Data Connector Page

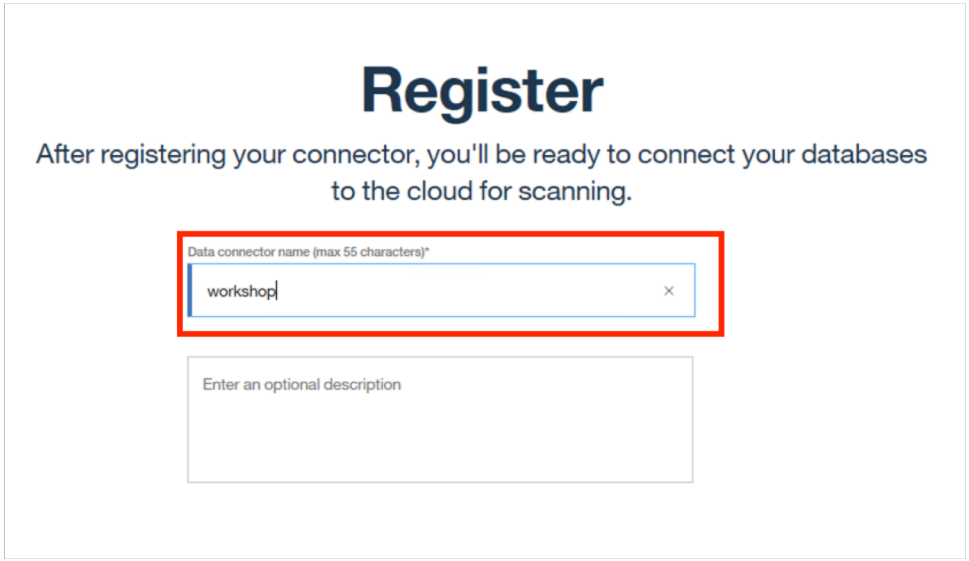


- After install, popup will ask if you would like to browse to the Data Connector page

Workshop: Connector Welcome Page

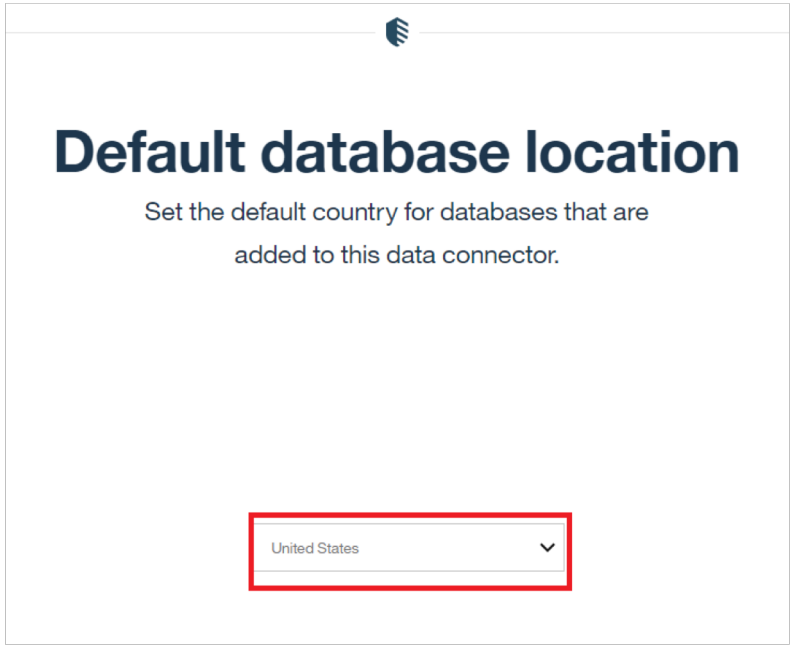


Workshop: Register Connector



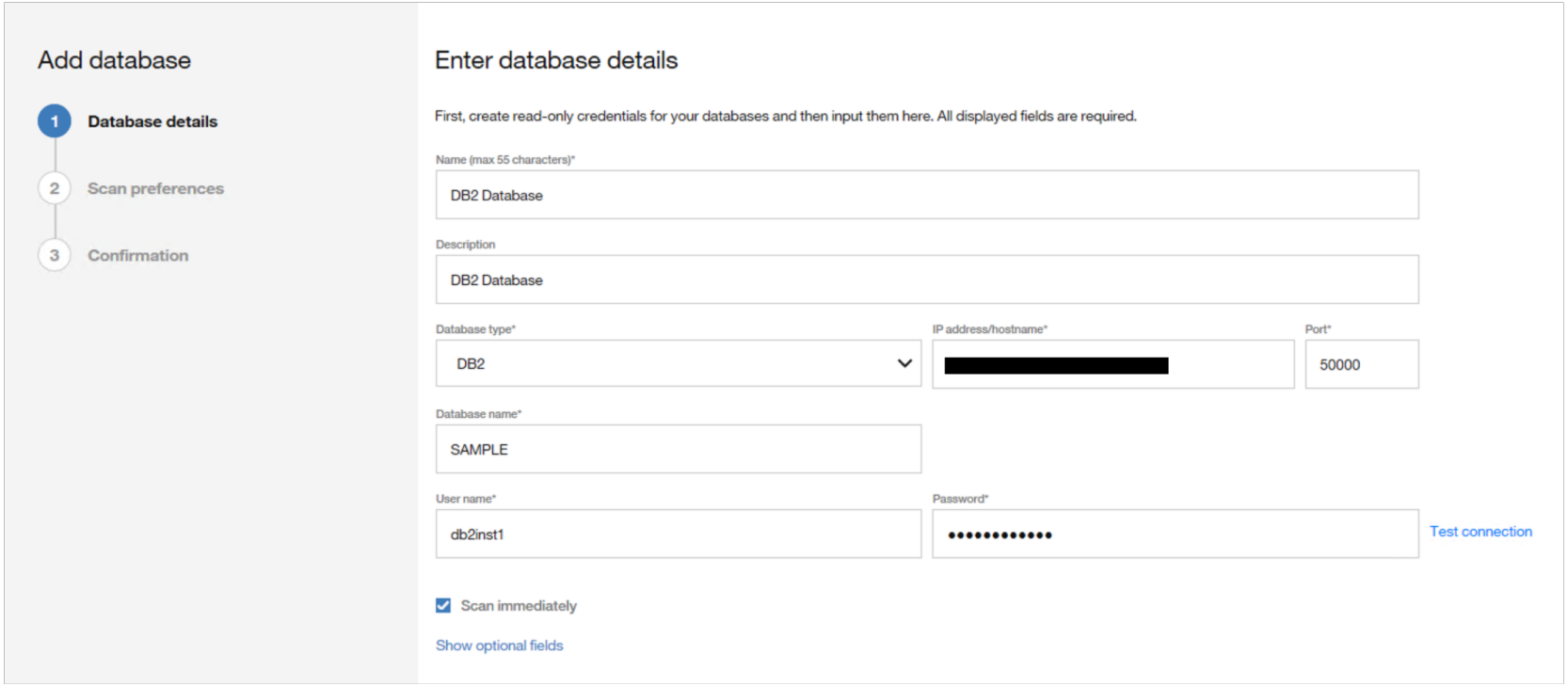
- **Fill in a unique name for this Data Connector**

Workshop: Default Location



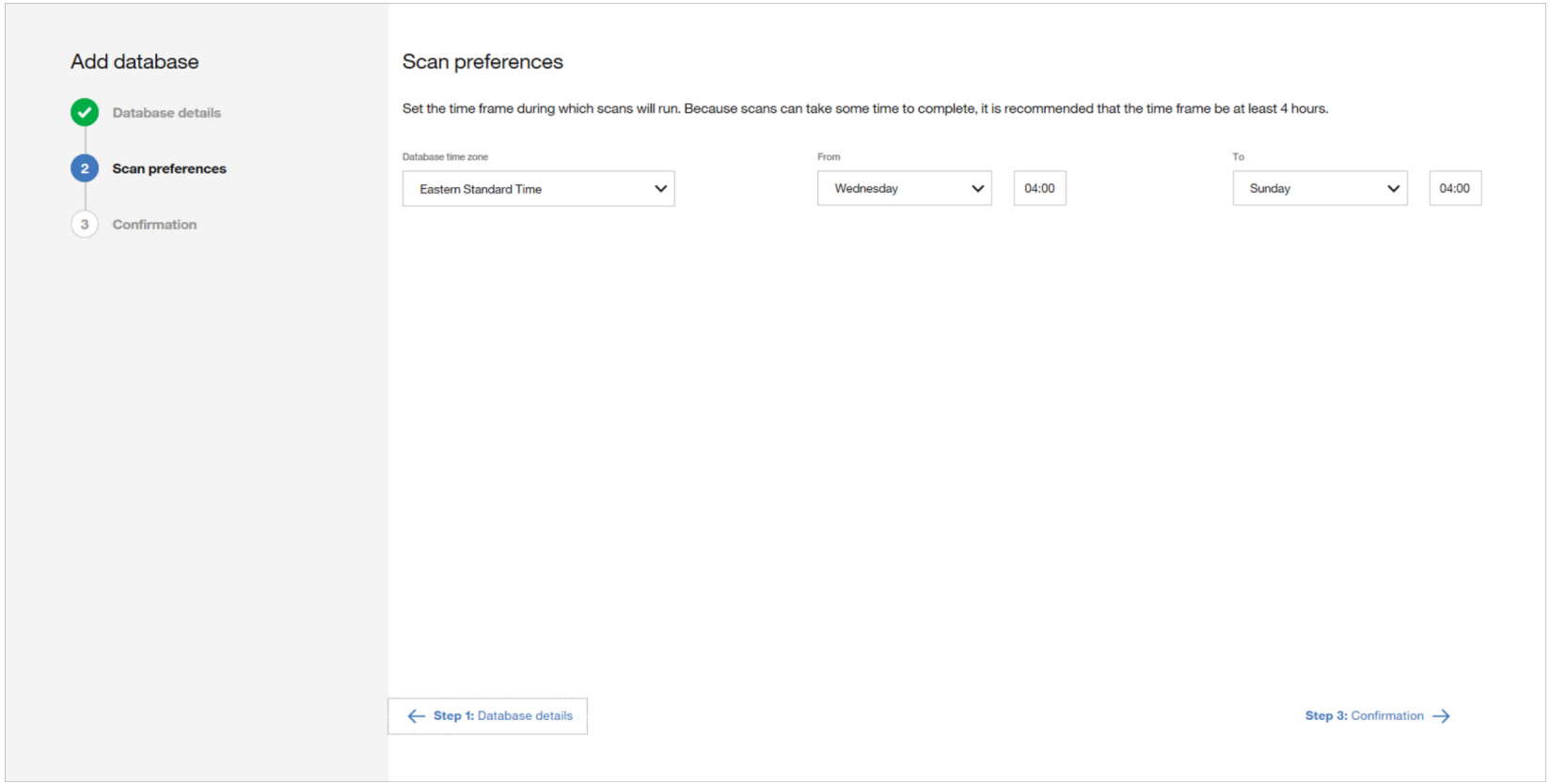
- **Select a default Country location that scanned databases will be identified in by Analyzer (useful for Map feature on Analyzer to see where all Databases are located)**

Workshop: Add Database to Scan



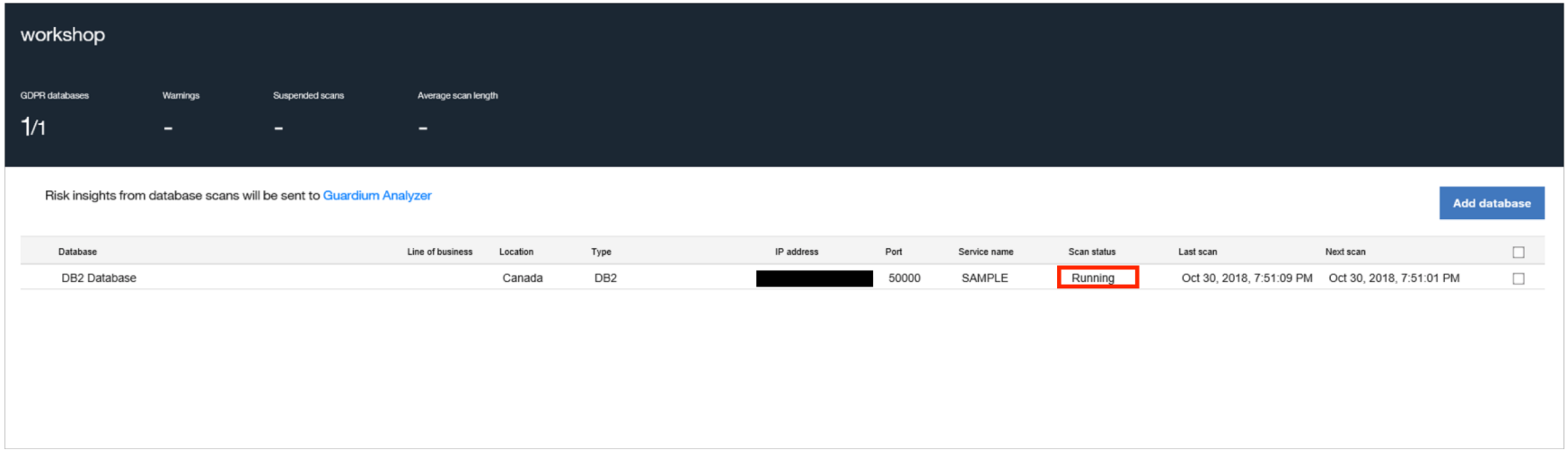
- **Fill in Database connection information and Country (if Country is not specified, will use Default Location given on previous page)**
- **Click “Test connection” to verify Connector can connect to Database**

Workshop: Scan Time Frames



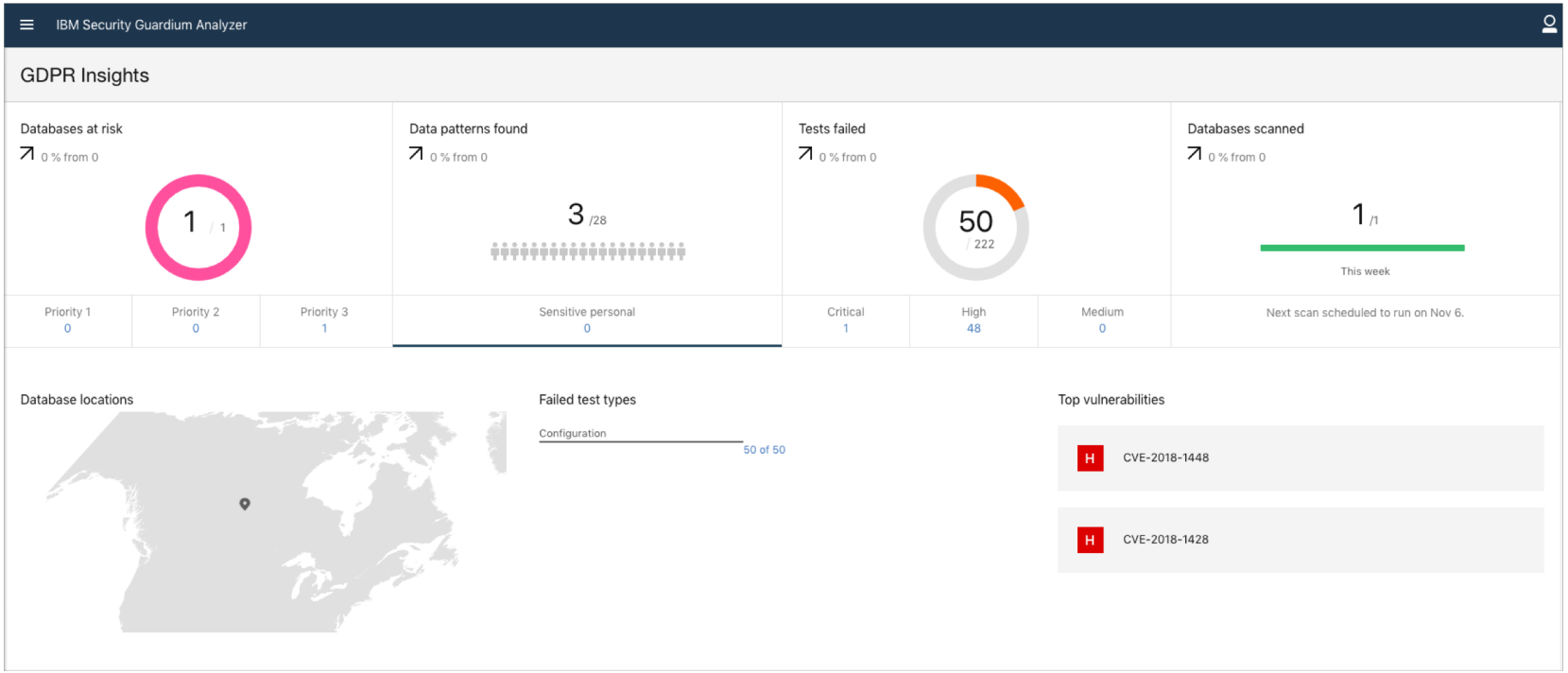
- **Specify what time frames are allowed for Connector to scan**

Workshop: Databases Page



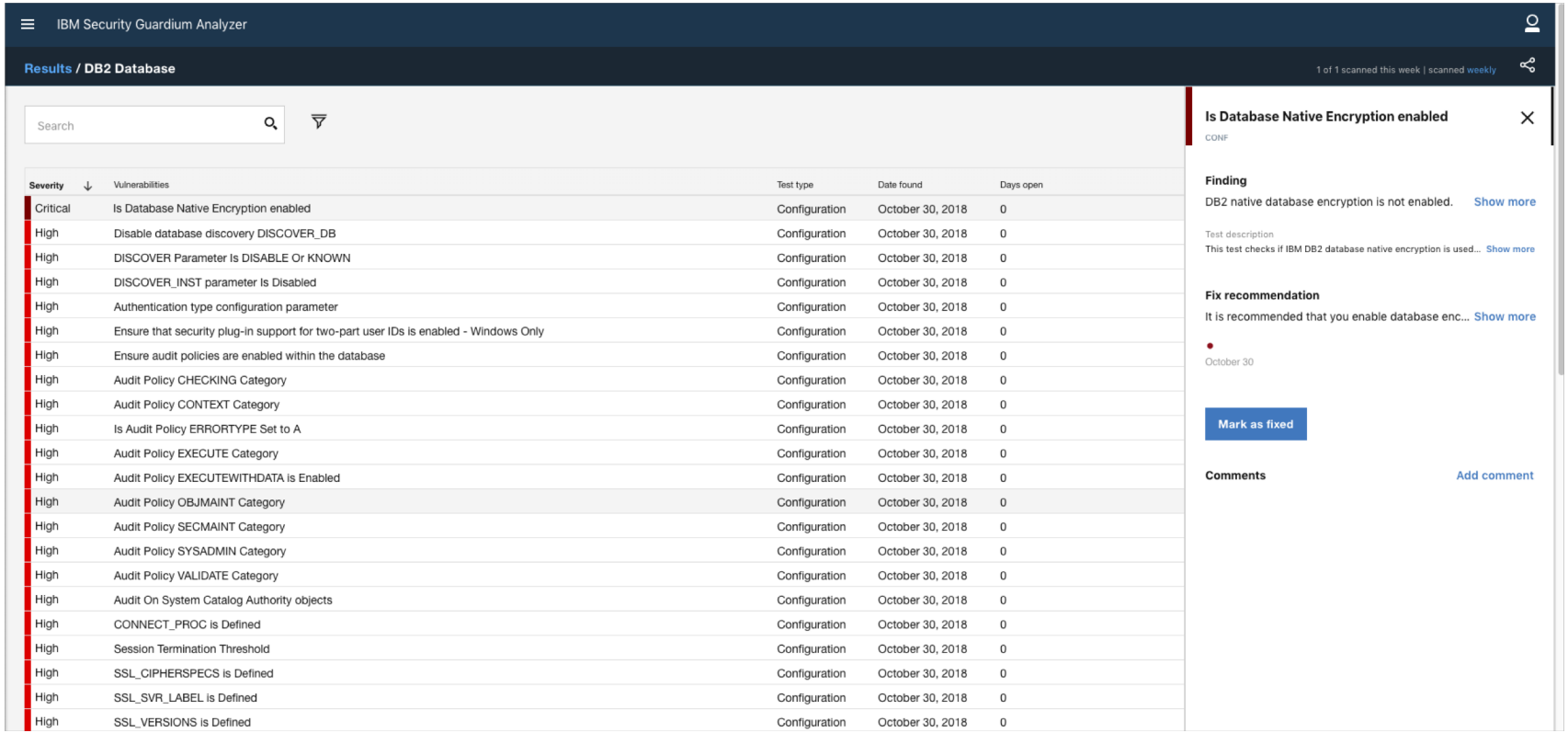
View and manage Databases on this Connector

Workshop: Back to Analyzer



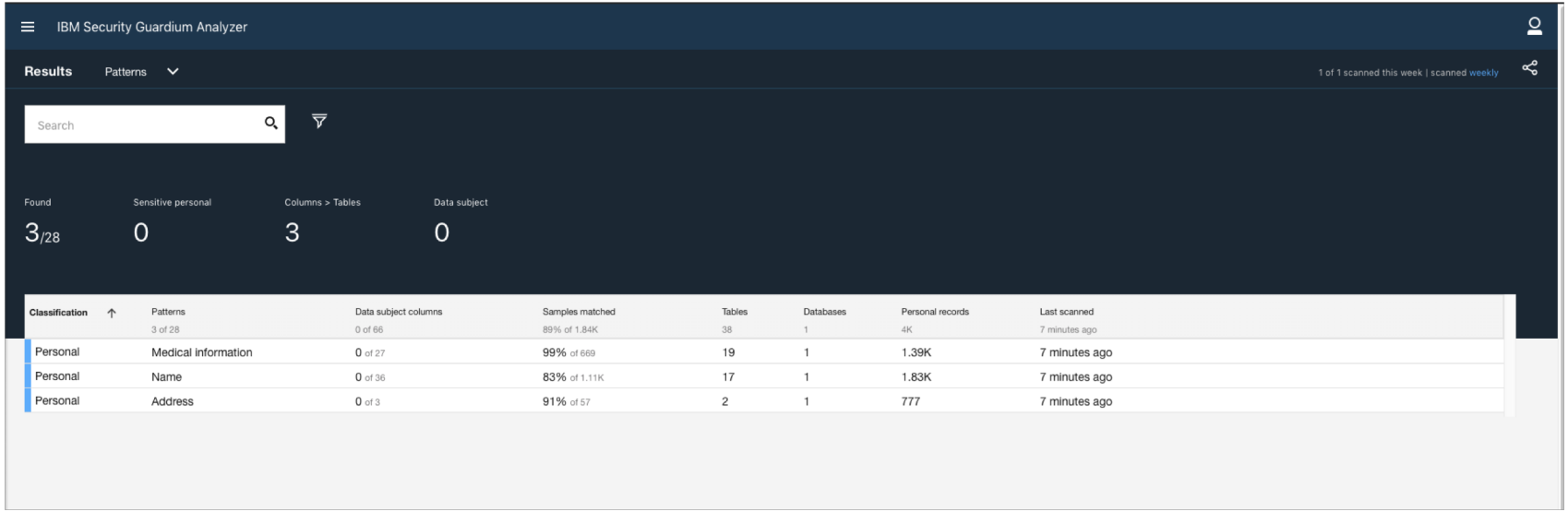
- **When returning to Analyzer home page, it will now show insights into the GDPR-relevant findings and risk of the added Database(s)**
- **Map feature will show locations of all Databases added to Connectors in your subscription**

Workshop: Database Vulnerabilities



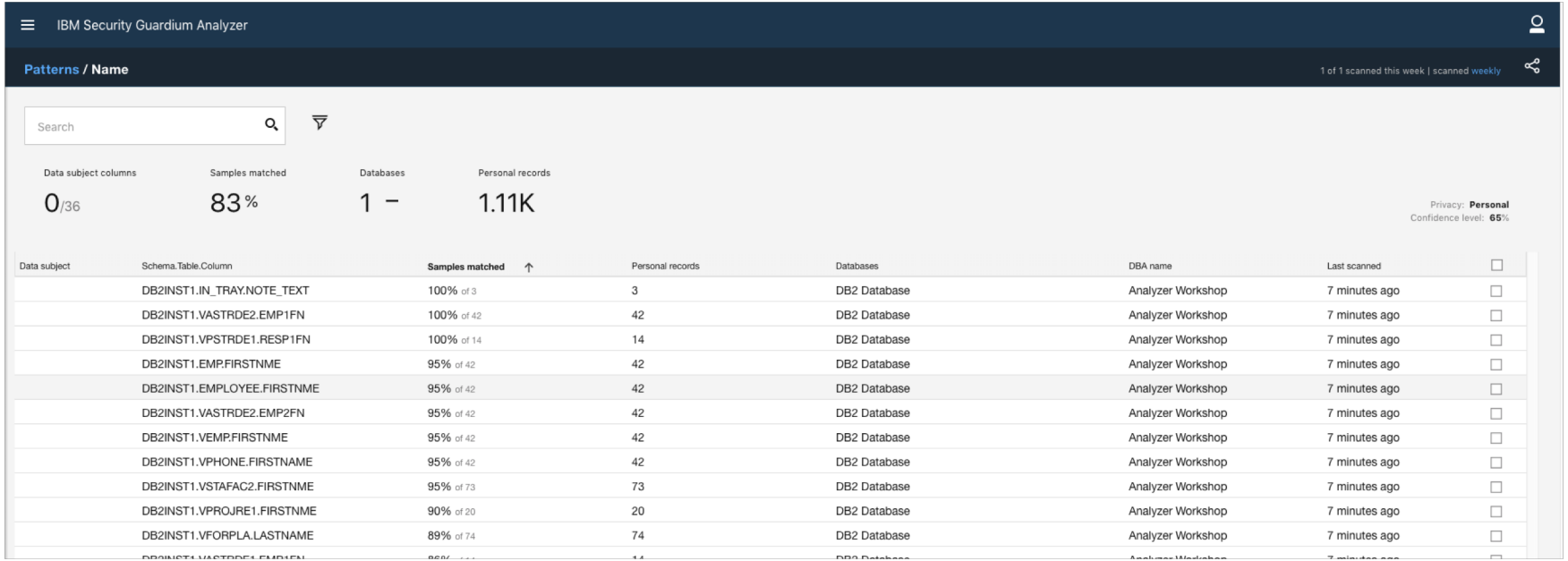
- View vulnerabilities on Databases and remediation recommendations
- Vulnerabilities are automatically sorted by highest severity

Workshop: GDPR-relevant Patterns Found



- View regulatory Patterns identified across Databases and number of records found
- Drill-down into any Pattern to view specific locations

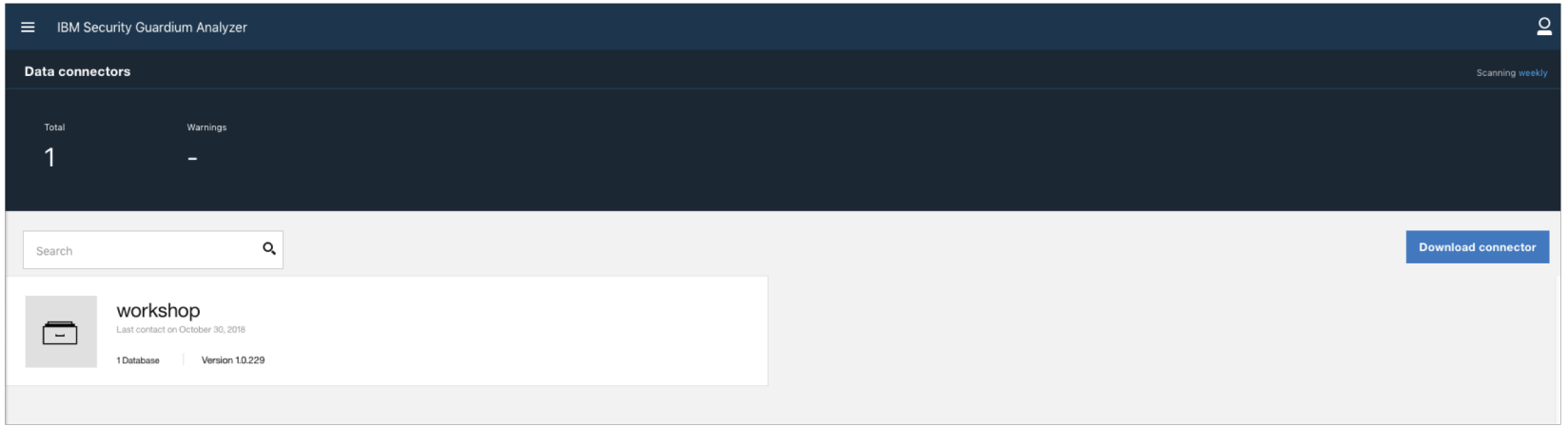
Workshop: Ex. Name Pattern Locations



Data subject	Schema.Table.Column	Samples matched	Personal records	Databases	DBA name	Last scanned
	DB2INST1.IN_TRAY.NOTE_TEXT	100% of 3	3	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VASTRDE2.EMP1FN	100% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VPSTRDE1.RESP1FN	100% of 14	14	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.EMP.FIRSTNME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.EMPLOYEE.FIRSTNME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VASTRDE2.EMP2FN	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VEMP.FIRSTNME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VPHONE.FIRSTNAME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VSTAFAC2.FIRSTNME	95% of 73	73	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VPROJRE1.FIRSTNME	90% of 20	20	DB2 Database	Analyzer Workshop	7 minutes ago
	DB2INST1.VFORPLA.LASTNAME	89% of 74	74	DB2 Database	Analyzer Workshop	7 minutes ago

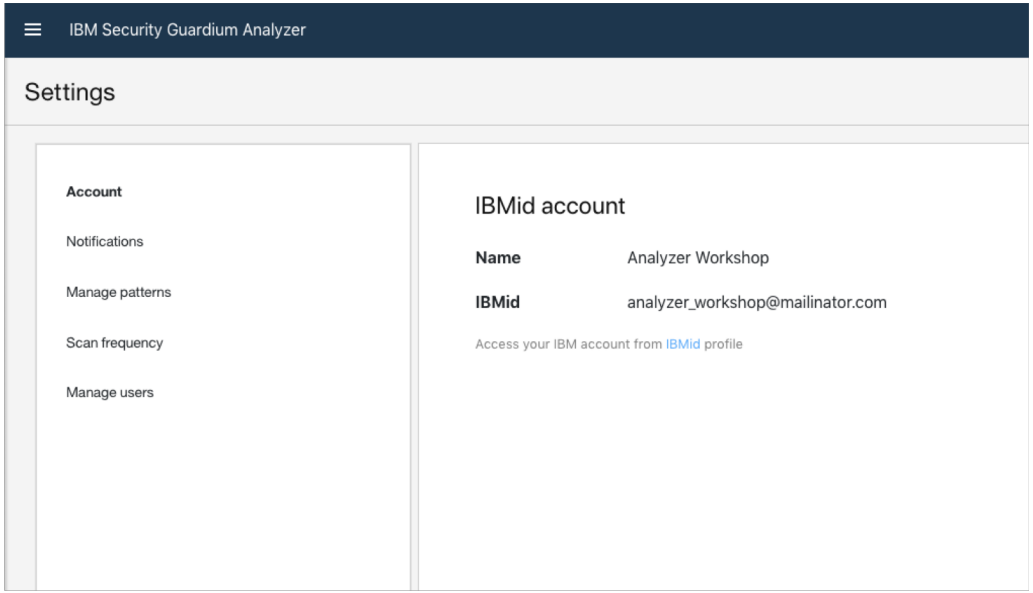
- **Drilled down into Name Pattern, for example**
- **View will include Schema, Table, Database, and Database owner (User who added the database) for each regulatory record found**

Workshop: Data Connectors Page



- **Connectors page to view all Connectors installed in the subscription, as well as a Download button to download Connectors in the future**

Workshop: Settings Page



- Change email notifications setting
- (Pro Accounts only) Add Patterns used to find regulatory data
- Adjust Scan Frequency
- Manage Users in Subscription

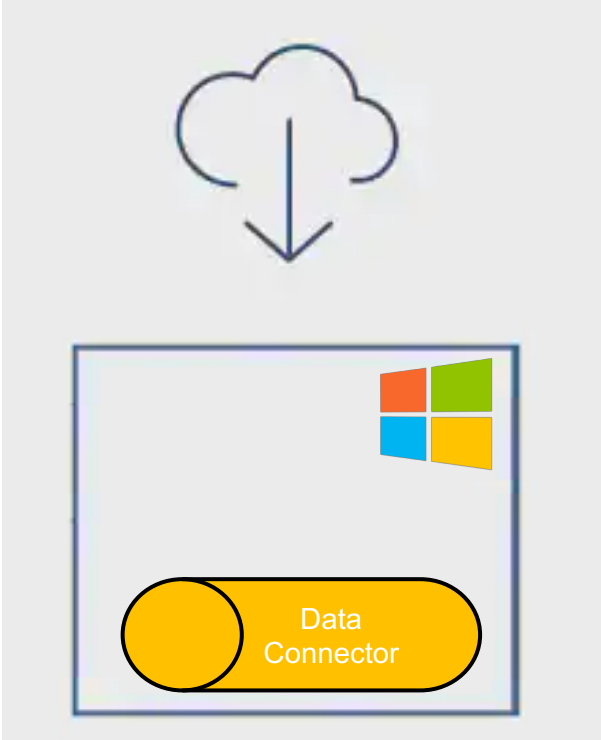
Maintenance

Maintenance: Cloud

- SaaS Offering
  - No Patching/Updating by Users
  - Continuous Delivery
  - Always using Latest Version

Maintenance: Data Connector

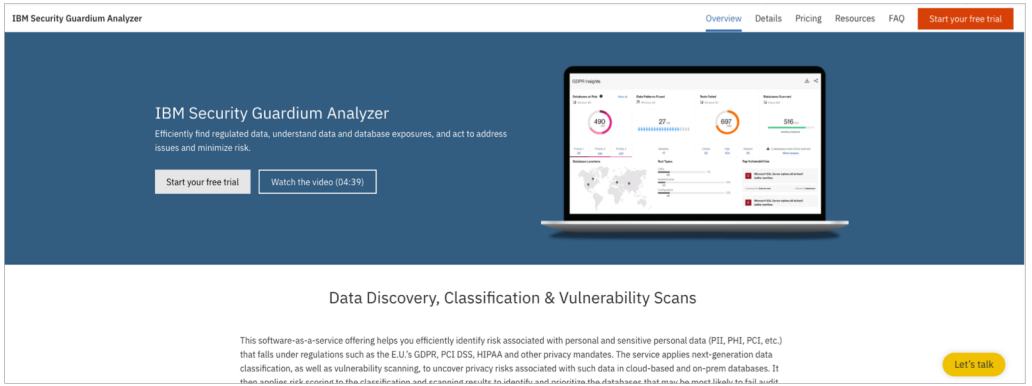
- **Windows Agent**
  - **Automatic Updates (in Background)**
  - **Regular Release of Data Connector**



Resources

Resources

- Guardium Analyzer marketplace page
  - View capabilities and subscription options
- Free trial
- Guardium Analyzer Data sheet
- Overview Guardium Analyzer demo video
- Product tutorial series:
  - Getting started with the Data Connector
  - Adding users to Guardium Analyzer
  - More to follow!
- Getting Started Guide/FAQ
- Webcast replay:
  After the GDPR Enforcement Date: Myths, Realities, and What to Do Now
- Webcast: "Analyzing Your GDPR Readiness: The Core Data Protection Capabilities You Need"



Devan Shah
Software Developer
IBM Data Security
devans@ca.ibm.com

Larry Lindsay
Senior Development Manager
IBM Security and Accessibility
llindsay@ca.ibm.com

IBM Security

Questions?

IBM

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM