Indonesia PDPL Compliance
Requirements

Data Breach Incident & Response Management

Enterprise Responsibility Under Indonesia PDPL Article 46

In the event of a failure to protect Personal Data, Data Controller is required to provide incident report

Notified to

- Personal Data Subject
- Indonesia Authority Committee

Within

3 x 24 hours

Minimum Contents

1. Details of Personal Data
2. Evidence of Data Breach
3. Handling and Remediation

Take a few minutes to quickly assess your organization readiness

Do you have clear visibility of data assets?

Do you have policy and procedure about data breach incident and response?

How do you log and monitor data accessibility across multiple data source?

How do you define and implement anomaly detection in data accessibility?

Are you struggling when processing data access log?

Unify. Simplify. Comply.

continuously across hybrid environments

Prevent
Detect
Continuous Compliance
Response
Evaluate

Key capabilities

Comprehensive Logs

Delivers complete, granular logging of all incoming and outgoing data access activities across databases. Ensuring compliance by quickly perform reconstruction of events and forensic analysis

Data Breach Alert

Enterprise can define thresholds or policies that automatically flag abnormal or high-risk data access behaviors. Machine-learning-based anomaly detection can also be done to detect potential breaches.

Automated Notification

Enabling rapid response and seamless integration with enterprise workflows. Ensuring stakeholders are informed immediately, accelerating containment and supporting compliance with strict time requirements.

Fulfillment of data breach and response management

Capture network information

Log

Collect activities from database client to database server and vice-versa which are:

Incoming:
- Client/server network connections
- Sessions (login/logout)
- SQL requests

Outgoing:
- SQL errors
- SQL result sets

Build policy and real-time anomaly detection

Alert

Define mechanism of real-time data breach detection and what actions must be taken to remediate that can be categorized as:

- Ordered Rules
- Risk Spotter
- Real-Time Trust Evaluator

Report incidents to stakeholders

Notification

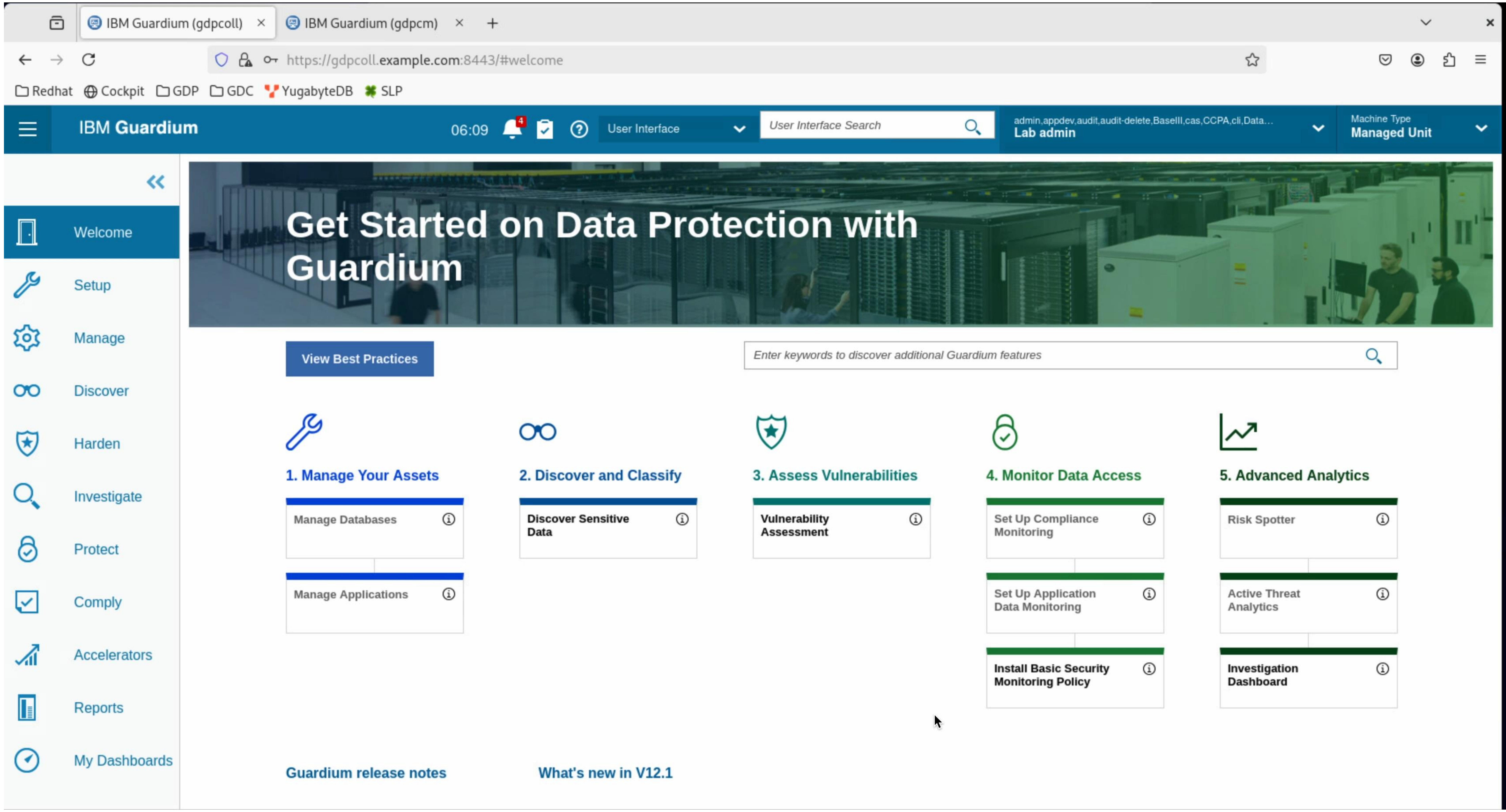
Create and send message to personal data subject and authority committee.

Message Content:
1) Details of personal data breach
2) Evidence (when and how)
3) Handling and remediation actions

Notification Mechanism:
1) SMTP/email
2) SIEM
3) Guardium notification
4) Other external systems or database

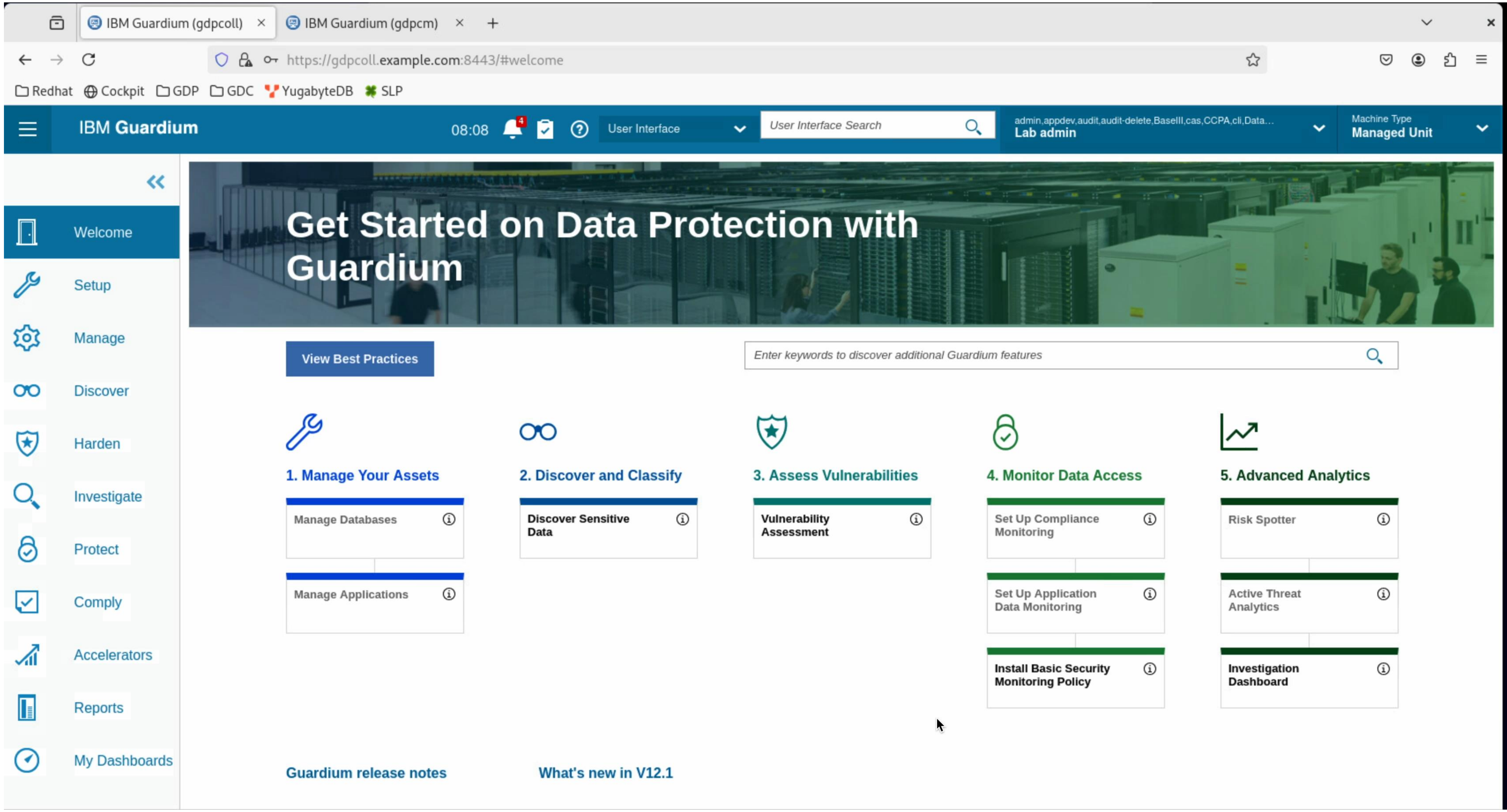
Demo

Policy Definition

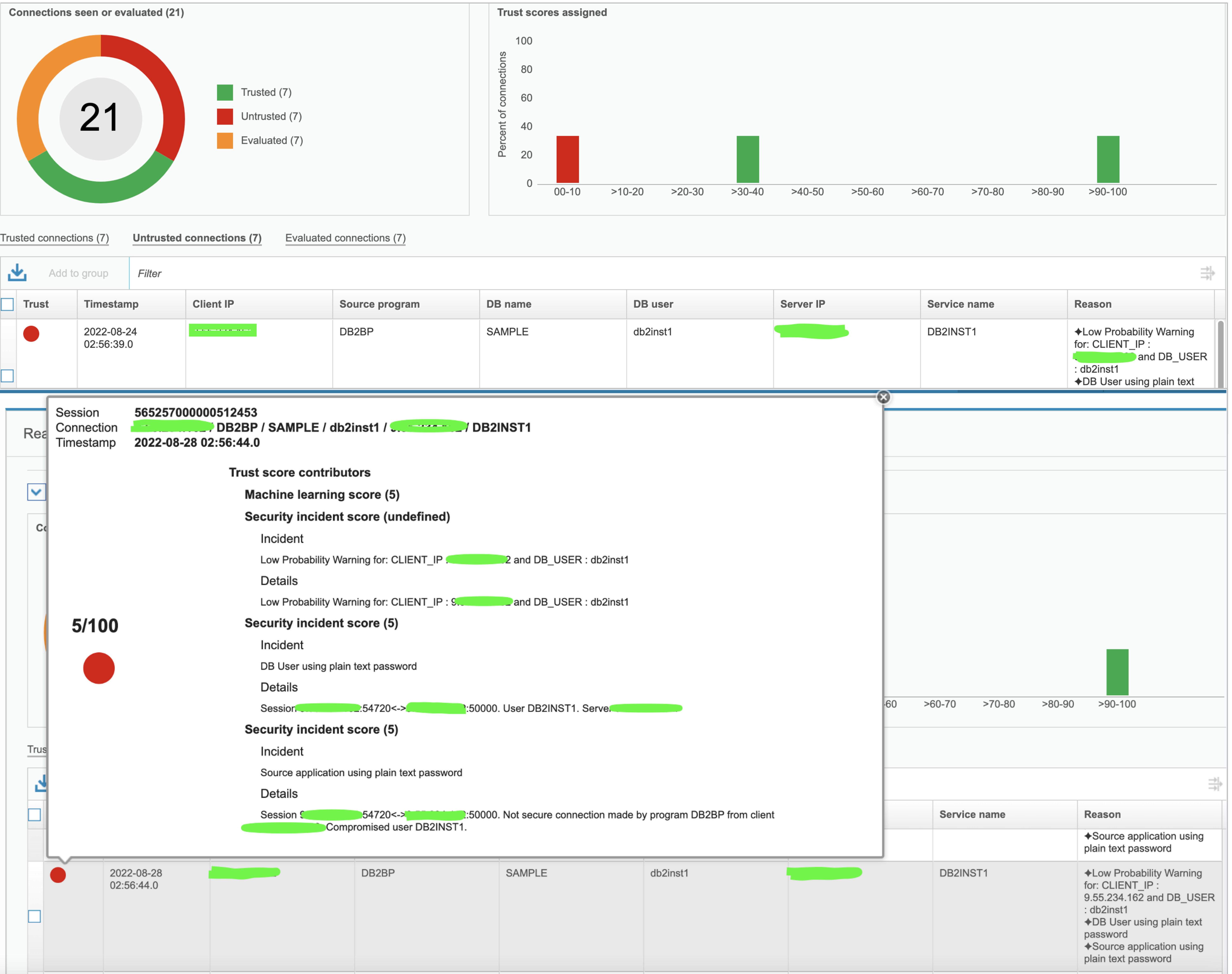


Demo

Alert Notification



Overview of Real-Time Trust Evaluator



Trusted connections (7) | **Untrusted connections (7)** | Evaluated connections (7)

□	Trust	Timestamp	Client IP	Source program	DB name	DB user	Server IP	Service name	Reason
□	●	2022-08-24 02:56:39.0	[redacted]	DB2BP	SAMPLE	db2inst1	[redacted]	DB2INST1	✦Low Probability Warning for: CLIENT_IP : [redacted] and DB_USER : db2inst1 ✦DB User using plain text

Session **565257000000512453**
Connection **[redacted] DB2BP / SAMPLE / db2inst1 / [redacted] / DB2INST1**
Timestamp **2022-08-28 02:56:44.0**

5/100

●

Trust score contributors

Machine learning score (5)

Security incident score (undefined)

Incident

Low Probability Warning for: CLIENT_IP [redacted] and DB_USER : db2inst1

Details

Low Probability Warning for: CLIENT_IP : [redacted] and DB_USER : db2inst1

Security incident score (5)

Incident

DB User using plain text password

Details

Session [redacted]:54720<->[redacted]:50000. User DB2INST1. Serve[redacted]

Security incident score (5)

Incident

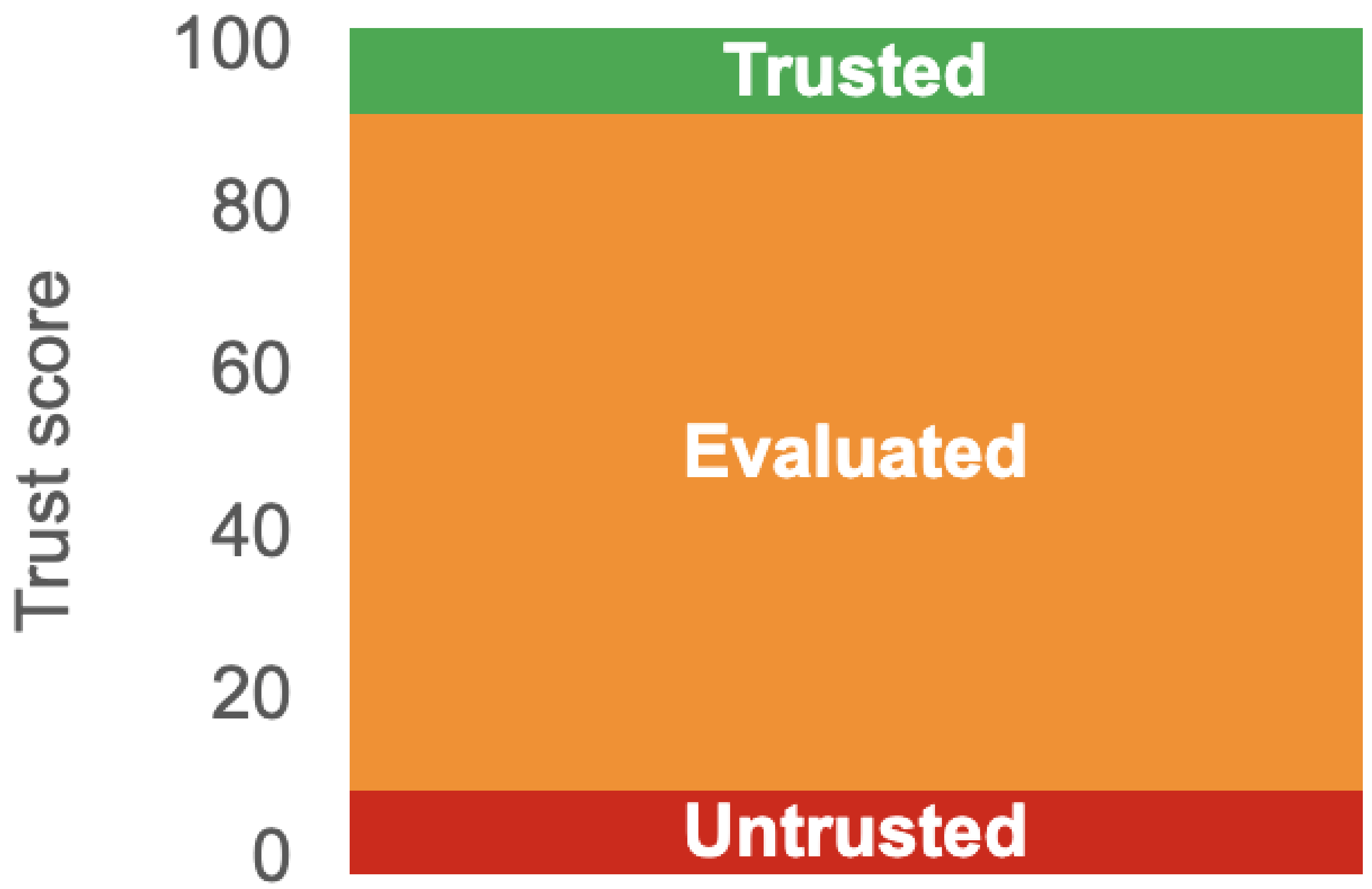
Source application using plain text password

Details

Session [redacted]54720<->[redacted]:50000. Not secure connection made by program DB2BP from client [redacted] Compromised user DB2INST1.

□	Trust	Timestamp	Client IP	Source program	DB name	DB user	Server IP	Service name	Reason
									✦Source application using plain text password
□	●	2022-08-28 02:56:44.0	[redacted]	DB2BP	SAMPLE	db2inst1	[redacted]	DB2INST1	✦Low Probability Warning for: CLIENT_IP : 9.55.234.162 and DB_USER : db2inst1 ✦DB User using plain text password ✦Source application using plain text password

Assess database connections and identifies security incidents using Realtime Security Incidents and Machine Learning Engines by generating **Trust Score**


Trust score
100
80
60
40
20
0
Trusted
Evaluated
Untrusted