CryptoPanel

edycja #29

Już za moment zaczynamy...

CryptoPanel

edycja #29

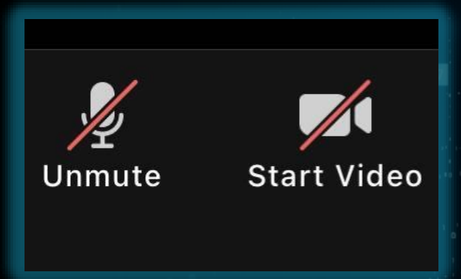
THALES
Building a future we can all trust

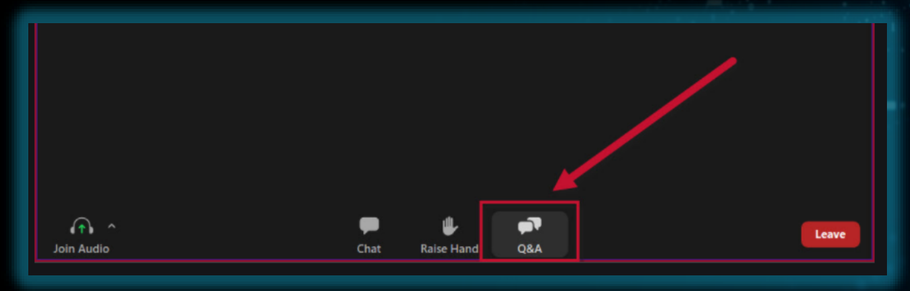
imperva
a Thales company

CLICO

CryptoPanel

edycja #29

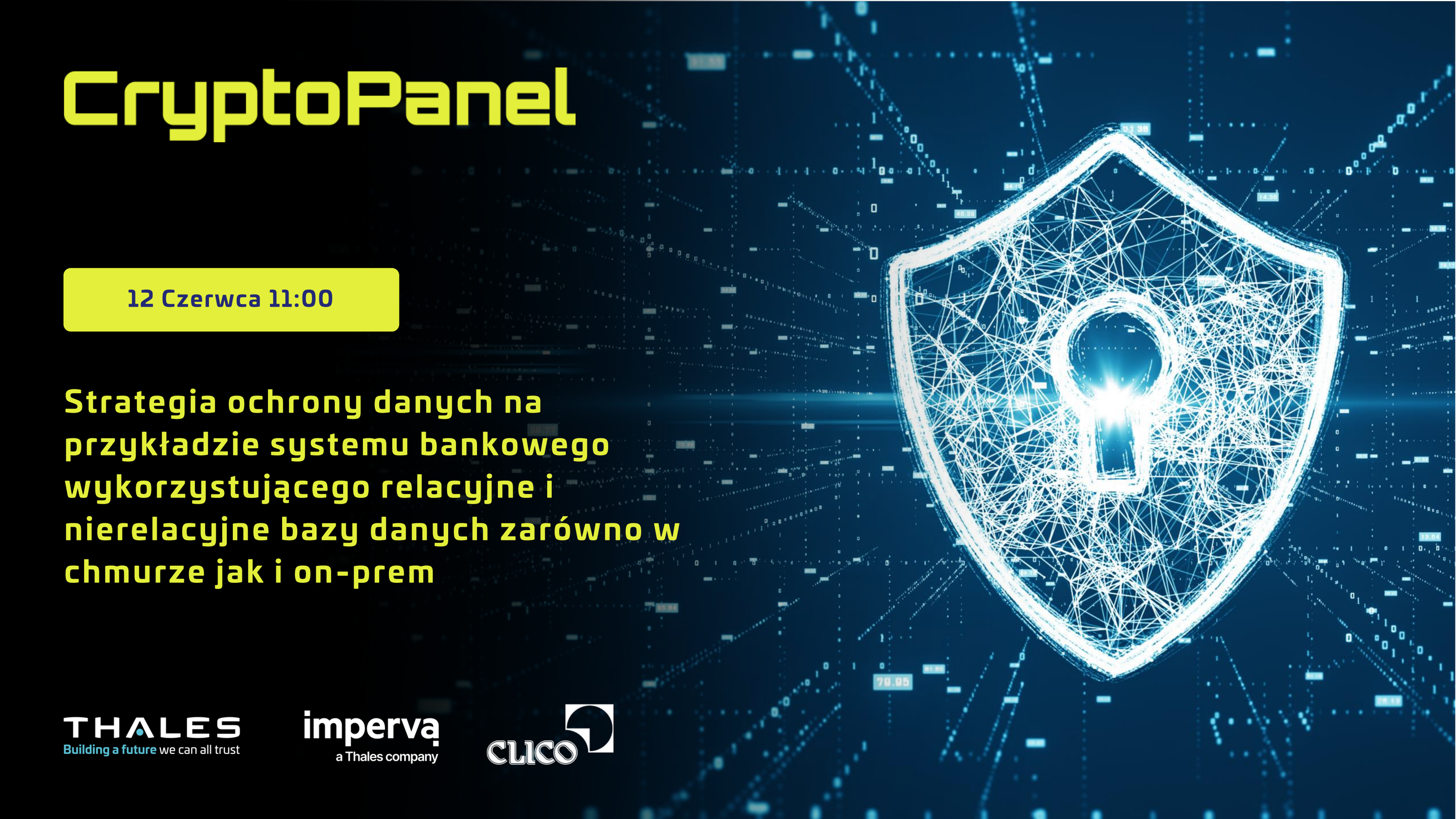




CryptoPanel

12 Czerwca 11:00

Strategia ochrony danych na przykładzie systemu bankowego wykorzystującego relacyjne i nierelacyjne bazy danych zarówno w chmurze jak i on-prem



THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel

TEST WIEDZY #29

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel

Dyskusje poprowadzą: Mateusz Paściak i Artur Holeczek

Mateusz Paściak

Pre-sales Engineer
mateusz.pasciak@clico.pl
mob. +48 605 445 593

Artur Holeczek

Partner Account Manager /
Product Manager
artur.holeczek@clico.pl
mob. +48 667 699 444

CryptoPanel

problem

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Nasze wyzwanie (czyli czelendże [*pisownia challenge*])

- **Potrzeba spójnego monitorowania istniejących baz danych I wykrywania nowych**
- **Nie widzimy co użytkownicy I admini baz danych właściwie robią na tych danych**
- **Potrzeba szybkiego udostępniania nowych funkcji dla klientów (technologia nie może być hamulcem biznesu) a istnieje problem z raportami dot. Compliance czy też zarządzaniem alertami w SOC**
  - zajmuje to za dużo czasu
- **Z perspektywy architektury problemem jest skalowanie. W środowisku jest 500 baz danych o bardzo dużej różnorodność silników np.**
  - MSSQL, Oracle, Snowflake, MongoDB, AWS RDS DynamoDB
  - Do tego ulokowane one są zarówno w on-prem czy jak widać w chmurach AWS, ale też jest Azure

- **Spójne podejście do bezpieczeństwa baz danych, ryzyka I zgodności**
- **Wgląd w to, kto, co, gdzie i w jaki sposób uzyskuje dostęp do krytycznych/wrażliwych zasobów**
- **Skalowalna architektura wspierająca bieżącą działalność i rozwój bazy danych**
- **Możliwość szybkiego wykrywania ryzykownych zachowań i reagowania na incydenty związane z bezpieczeństwem**
- **Scentralizowane monitorowanie i widoczność wrażliwych danych i luk w zabezpieczeniach, których właścicielem jest dział bezpieczeństwa, a nie zespół DBA**
- **Możliwość tworzenia raportów zgodności w ciągu kilku minut**

CryptoPanel

rozwiązanie

THALES
Building a future we can all trust

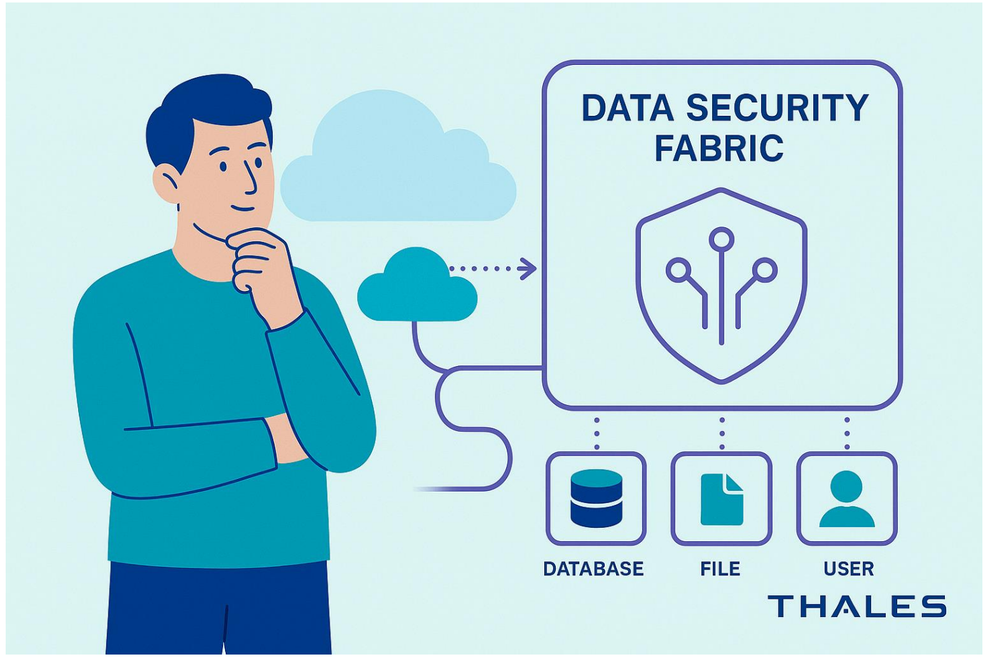
imperva
a Thales company

CLICO

Czym jest właściwie DSF – Data Security Fabric?

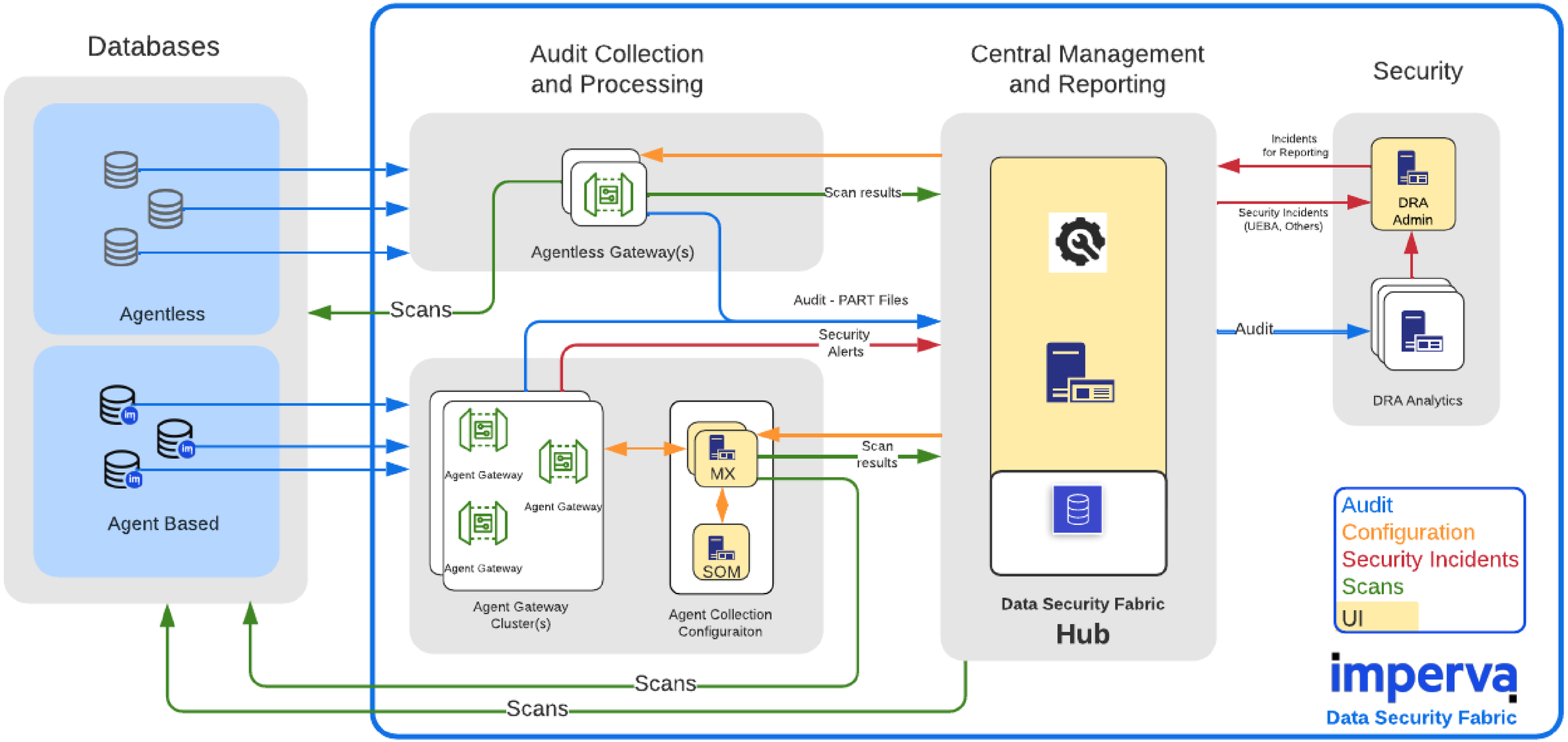
Krótkie wprowadzenie:

- DSF to tak naprawdę robiąca wrażenie fajna nazwa koncepcji, która nie wyraża konkretnych systemów jak WAF, DAM, HSM itd., z czego to wynika?
- Pod spodem DSF kryją się tak naprawdę 3 inne systemy, które połączone w całość tworzą to co nazywa się DSF:



- **DAM** od Database Activity Monitoring czyli klasyczne podejście firmy Impervy do zbierania audytu z baz danych w sposób agentowy (zewnętrzny soft na silniku bazy danych) zazwyczaj w on-prem
- **DSF HUB** historycznie jSonar potem Sonar... realizujący podobne założenia co DAM czyli zbieranie logów audytowych z naszych baz ale w sposób bezagentowy a więc mowa o natywnym audycie, szczególne zastosowanie to bazy w chmurze np. będące usługą zarządzaną do której agenta nie da się dostawić
- **DRA** czyli Data Risk Analytics realizujący m.in. zaawansowane funkcjonalności UEBA (identyfikacja zachowań użytkowników), po to aby powiedzieć czy ktoś nie narusza bezpieczeństwa danych.

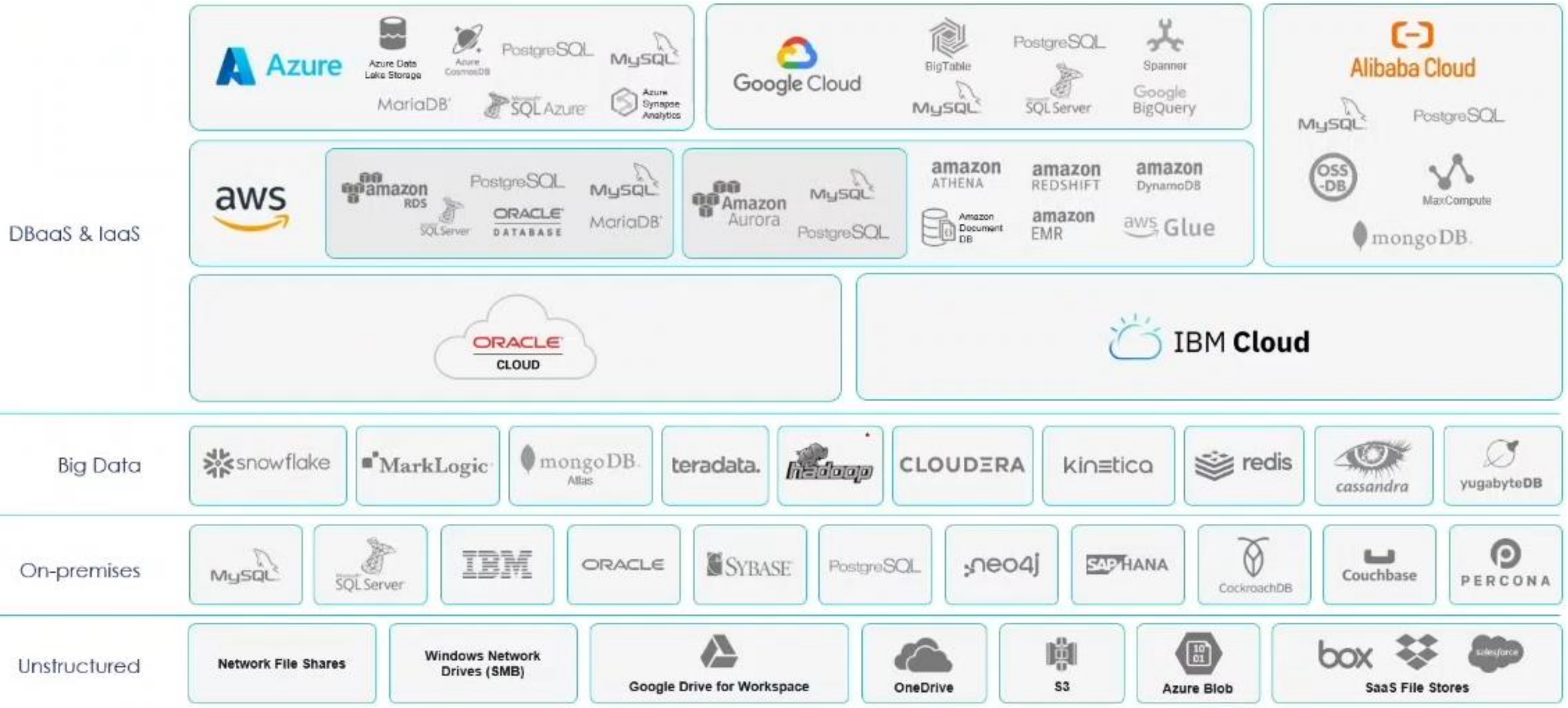
THALES



THALES

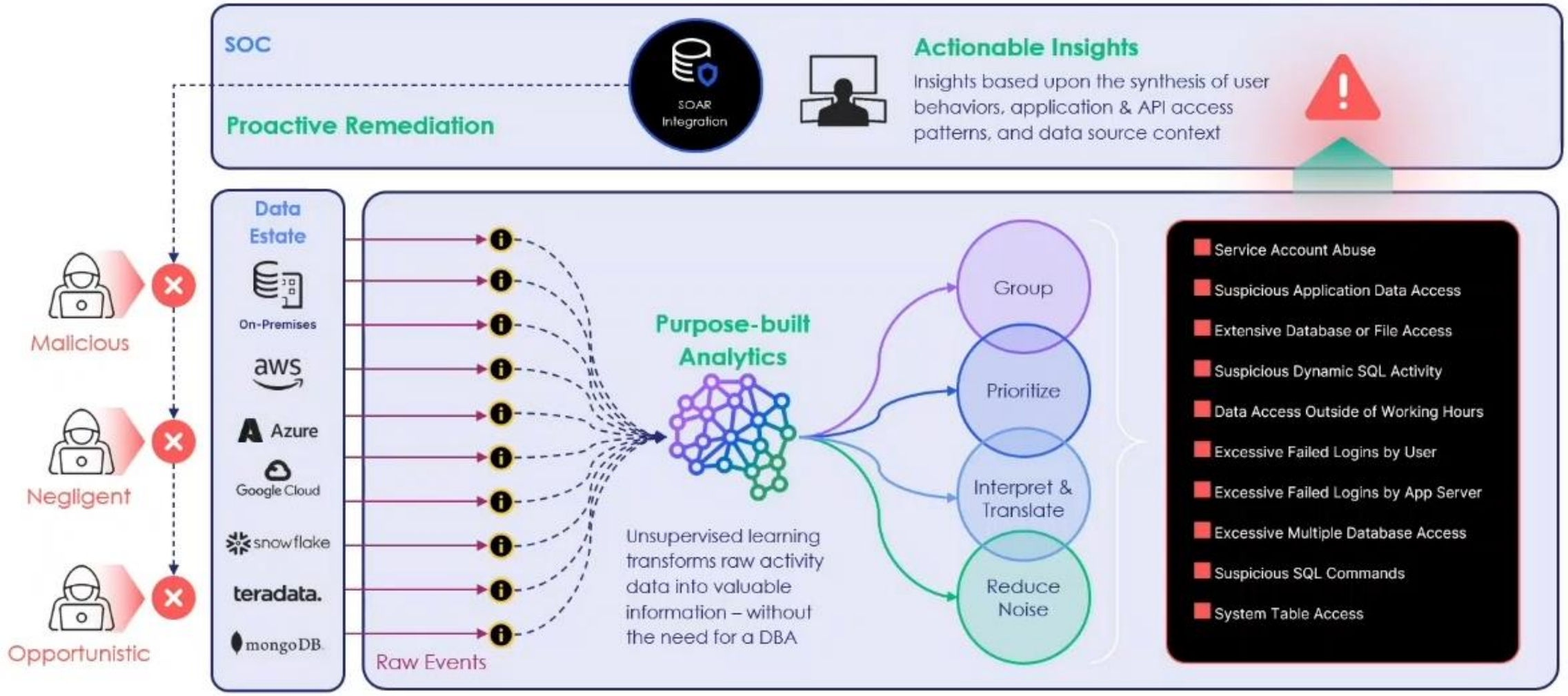
Ochrona dla różnych źródeł i typów danych

Structured, semi-structured, and unstructured



DRA – Data Risk Analytics

DRA can be the home page for data security in your SOC



Kategorie incydentów w DRA

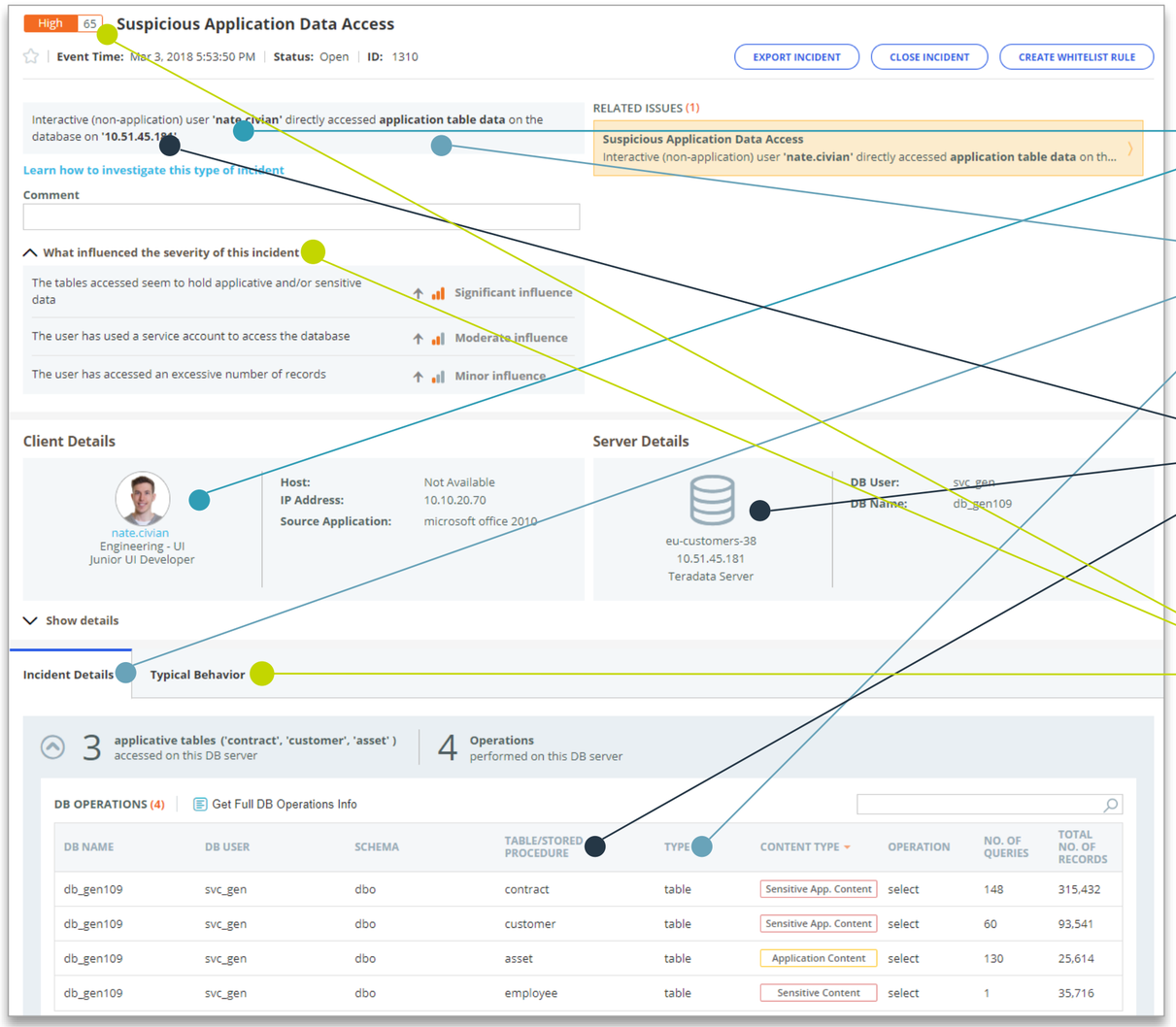
4 Hours update intervals

- Active Attack on Database - Audit Tampering
- Active Attack on Database - Command Execution
- Active Attack on Database - Credentials Extraction
- Active Attack on Database - Data Exfiltration
- Active Attack on Database - Database Weaponization
- Active Attack on Database - Malware Deployment
- Active Attack on Database - OS File Read
- Active Attack on Database - Privilege Escalation
- Active Attack on Database - Ransomware
- ...and more

24 Hours interval update

- Database Access at Non-standard Time
- Database Service Account Abuse
- Excessive Database Record Access
- Excessive Failed Logins
- Excessive Failed Logins from Application Server
- Excessive Multiple Database Access
- Machine Takeover
- Suspicious Application Data Access
- Suspicious Database Command Execution
- Suspicious Dynamic SQL Activity
- Suspicious OS Command Execution
- Suspicious Sensitive System Tables Scan
- ...and more

Przykład użycia DRA w praktyce



WHO?

WHAT?

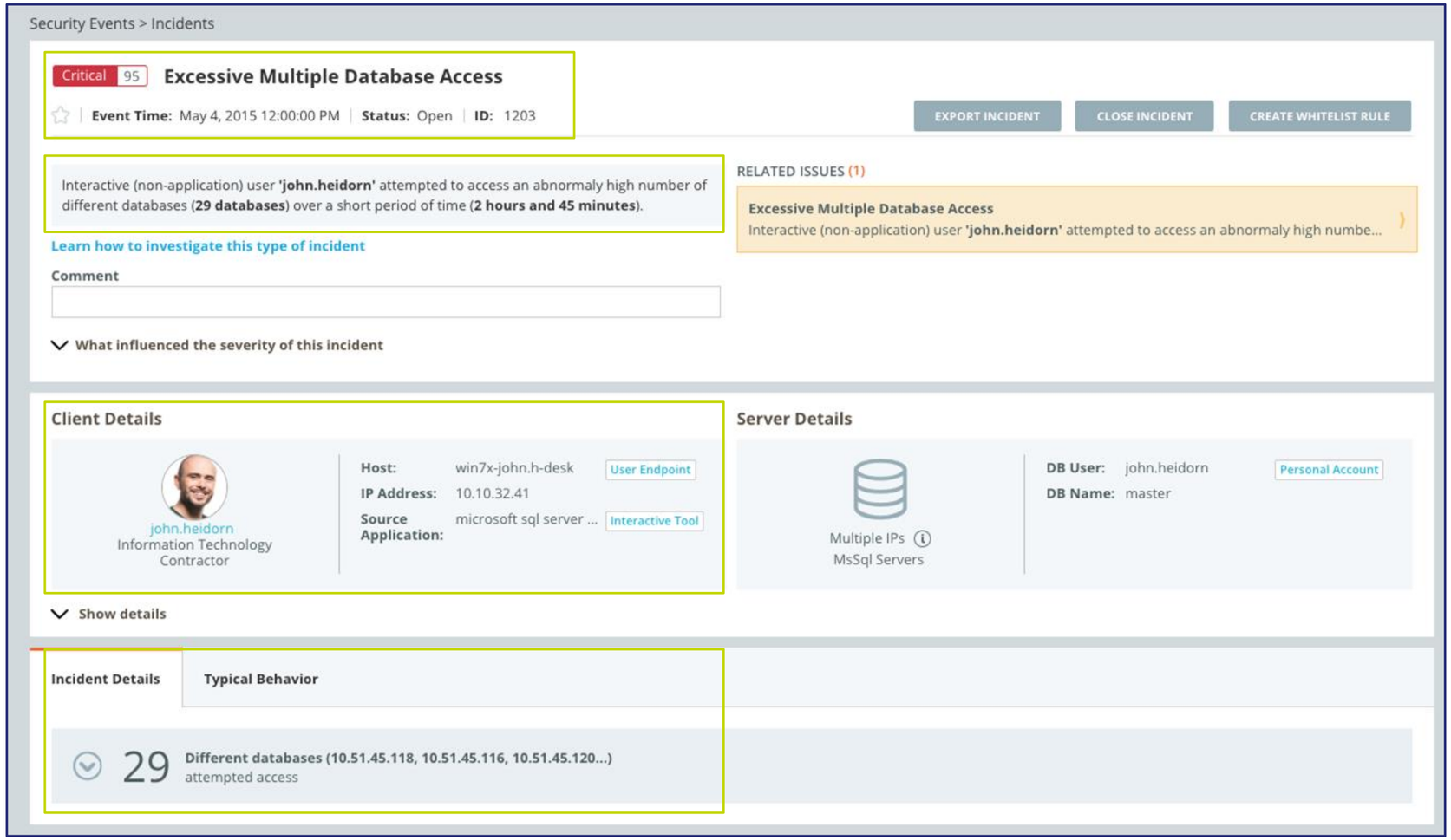
WHERE?

IS IT OK?

Out-of-the-box, extensible models for:

- Suspicious Data Change
- Suspicious Data Access
- Suspicious Connections
- Super Users and Verb Categories
- Service Account Abuse
- Suspicious Grants
- Suspicious Account Creation
- Suspicious Data Unload
- Suspicious Command Usage / Injection
- Suspicious Character Usage
- SQL Injection
- Machine Takeover Propagation
- Machine Takeover Breakout Attempt
- Brute Force Login Attacks
- Nonstandard Login Times
- Nonstandard Access Times
- Excessive SQL Error against Sensitive Objects
- Excessive Data Modifications
- Excessive Data Extrusion
- Excessive Connections
- And more..

Kolejny przykład DRA



- The user attempted to access 29 different DBs over a short period of time.
- Prioritize what matters the most.
- Interpret security incident in plain language.

Incident Details | Typical Behavior

TYPICAL DAILY DB RECORD ACCESS

In comparison to the 1,178,000 records accessed in this event

TYPE	NAME	DAILY AVERAGE (RECORDS/DAY)	DAILY'S 90TH PERCENTILE (RECORDS/DAY)
User	john.heidorn	9,000	14,000
Department	it	10,000	15,000
Organization		15,615	23,049

Source Details

john.heidorn (Information Technology)
Contractor

Host: win7x-john.h-desk
IP Address: 10.10.32.41
Source Application: aqua_data_studio

Destination Details

Oracle

Dest IP: 10.10.194.32
DB User: hydra
DB Name: dnaweb

Incident Details | Typical Behavior

1,178,000 **Records** accessed from 2 tables | 2 **Operations** performed on this DB server

Critical 95 **Active Attack on Database - Audit Tampering**

Event Time: Jul 28, 2022 2:39:05 PM | **Status:** Open | **ID:** 2730

Close incident | Create Allow List

The database has been actively attacked. The attacker attempted to truncate, drop or delete audit data stored in the audit tables "AUDSYS.AUD$UNIFIED" or "SYS.AUD$", and most probably still has access to the database and may continue to execute various attacks.

Learn how to investigate this type of incident

Comment

What influenced the severity of this incident

Source Details

mariam.harris (Information Technology)
Manager

Host:	win7-harris.m
IP Address:	10.10.32.41
Source Application:	datagrip

Destination Details

Oracle

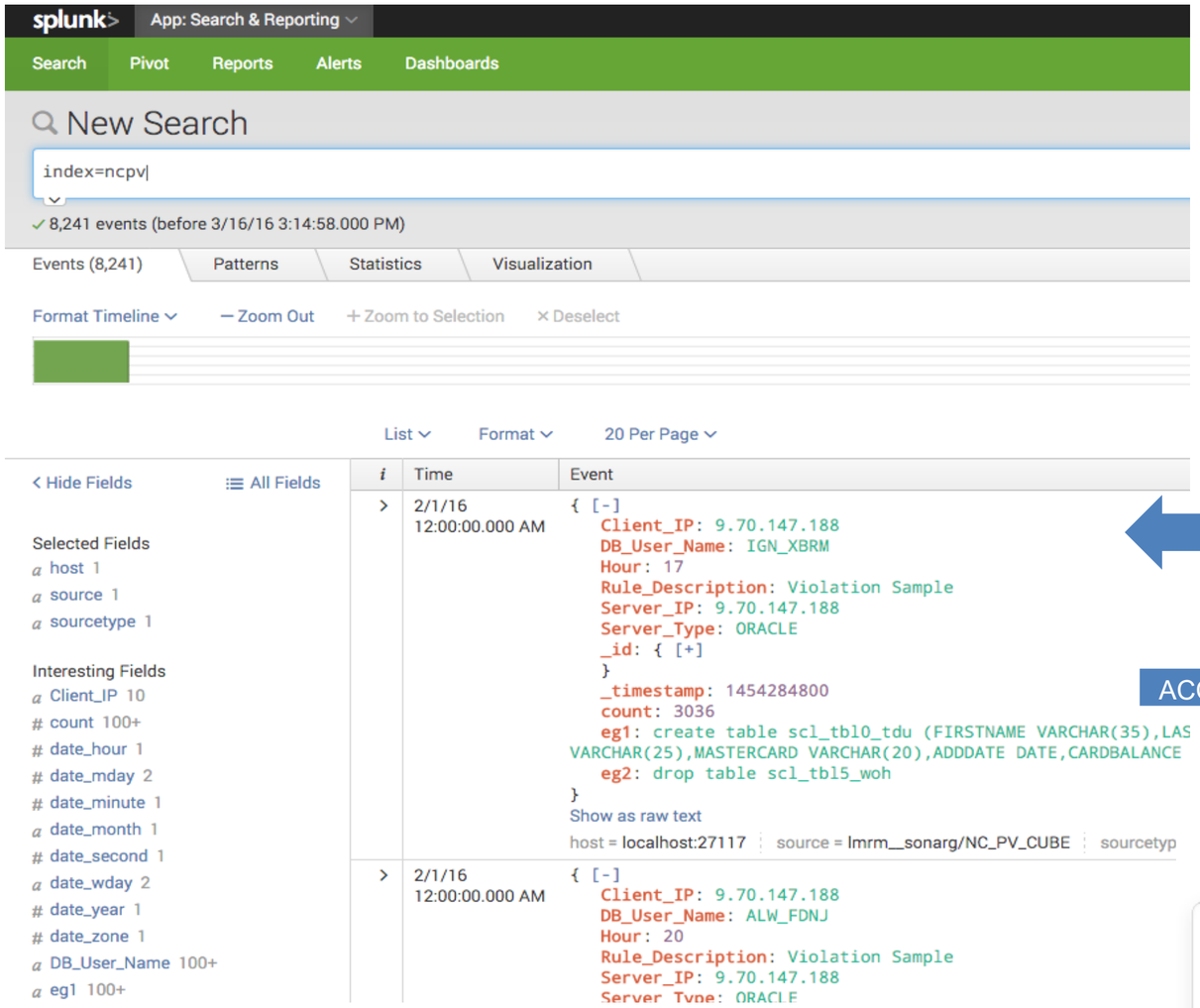
Host:	SecResOracle19Linux0
Dest IP:	10.100.184.18
DB User:	system
DB Name:	orcl

Incident Details

SQL commands that triggered the attack:

Timestamp	Query
2021-11-30T12:39:05+0000 - 0	truncate table sys.aud$
2021-11-30T12:39:05+0000 - 1	truncate table audsys.aud$unified
2021-11-30T12:39:05+0000 - 2	drop table sys.aud$
2021-11-30T12:39:05+0000 - 3	drop table audsys.aud$unified

Wzbogacanie danych i redukcja szumu na przykładzie integracji ze Splunk



Reduce Splunk costs without compromising access to the data or the user experience

- Queries can be run in Splunk without having to index the data
- Keep the raw data in jSonar and pass summary/aggregated data
- The user experience is as if it's in Splunk

RAW DATA

ACTIONABLE/ENRICHED EVENTS

ACCESS TO ANY DATA OVER VIRTUAL INDEX

METADATA

imperva Sonar

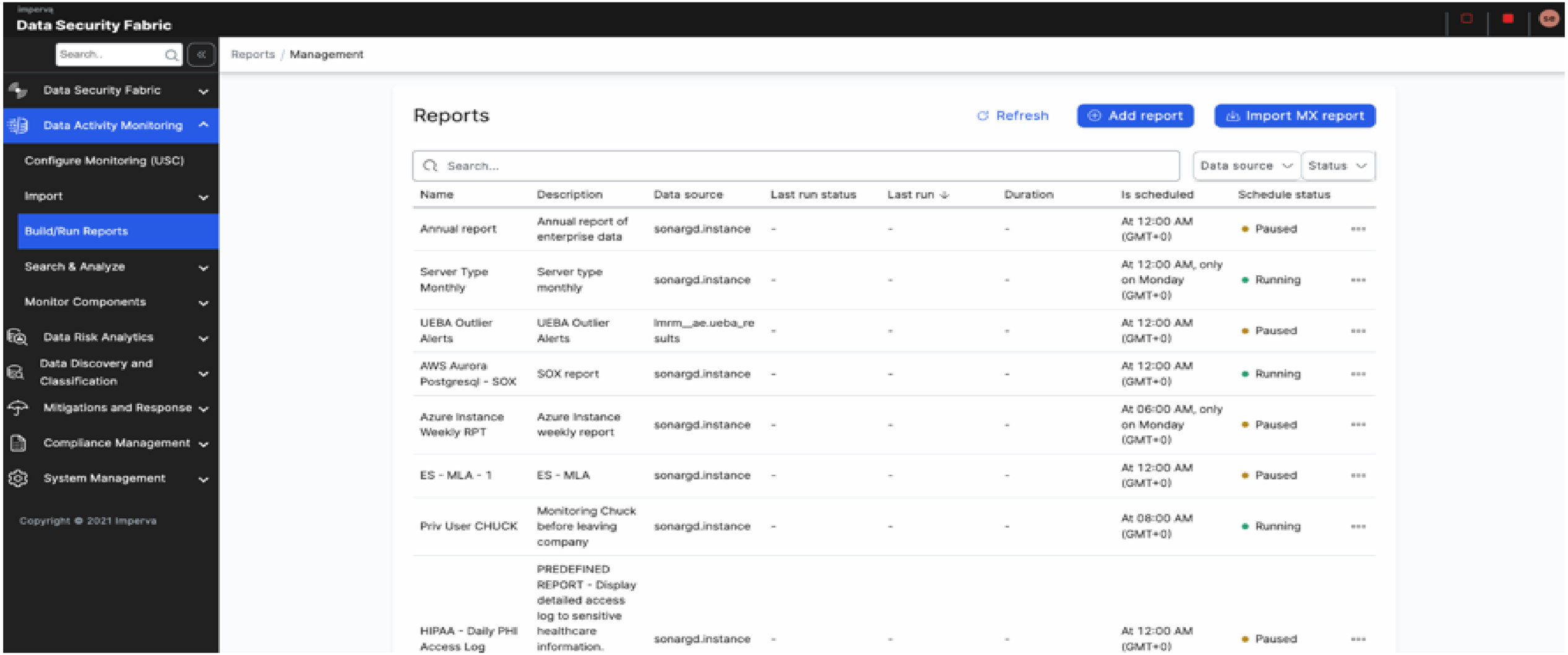
SQL Collection

```
SELECT * FROM Accounts
WHERE AccountNbr LIKE
%1234*%
```

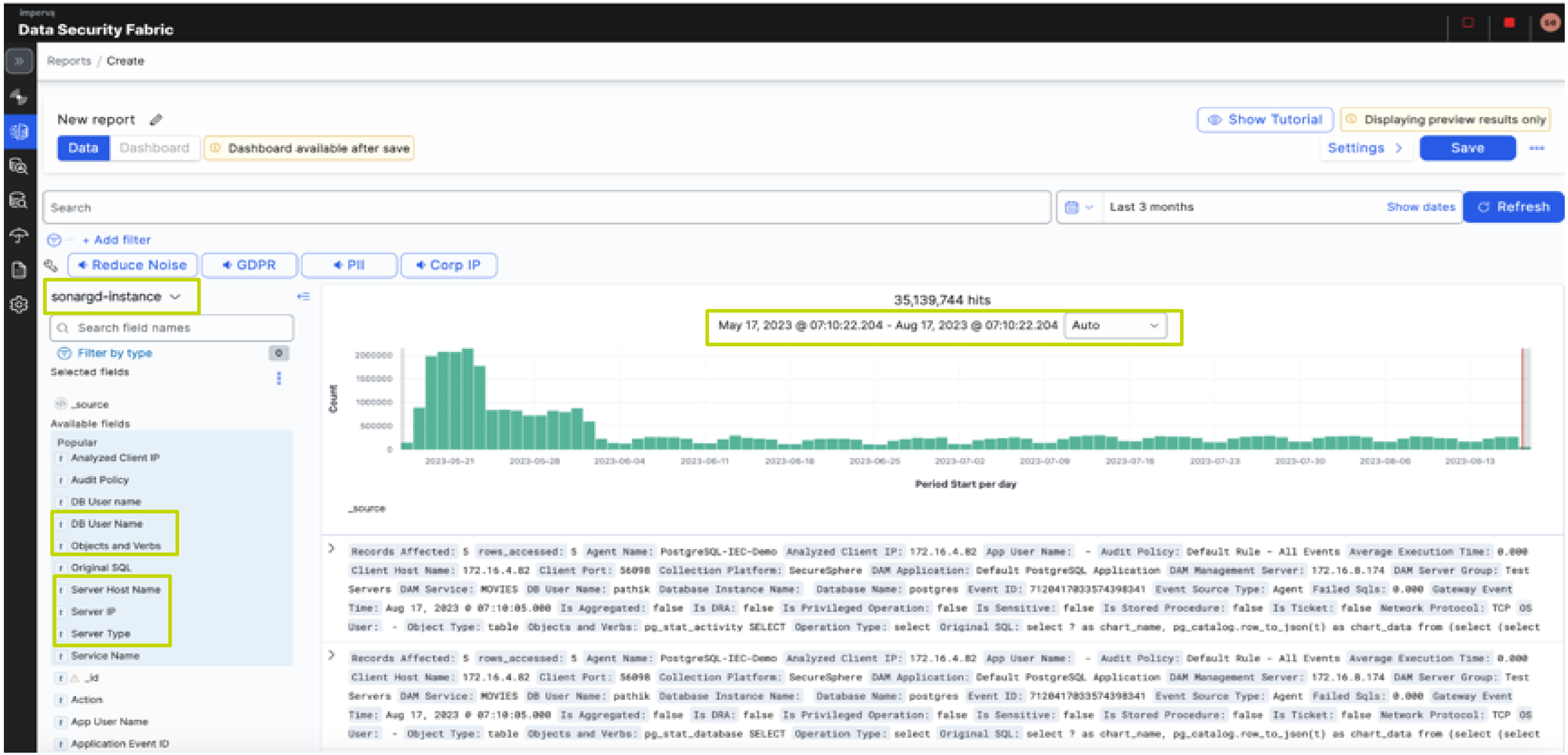
SQL transformed with imperva Data Security Fabric analytics

User: Joe	Column: AccountNbr
Type: Human	Content Type: Sensitive
Source: 42.24.1.3	Operation: Select/View
Dest: Master DB	Queries: 50
Type: Table	Records: 1,567,000
Table/SP: Accounts	Behavior: Unusual

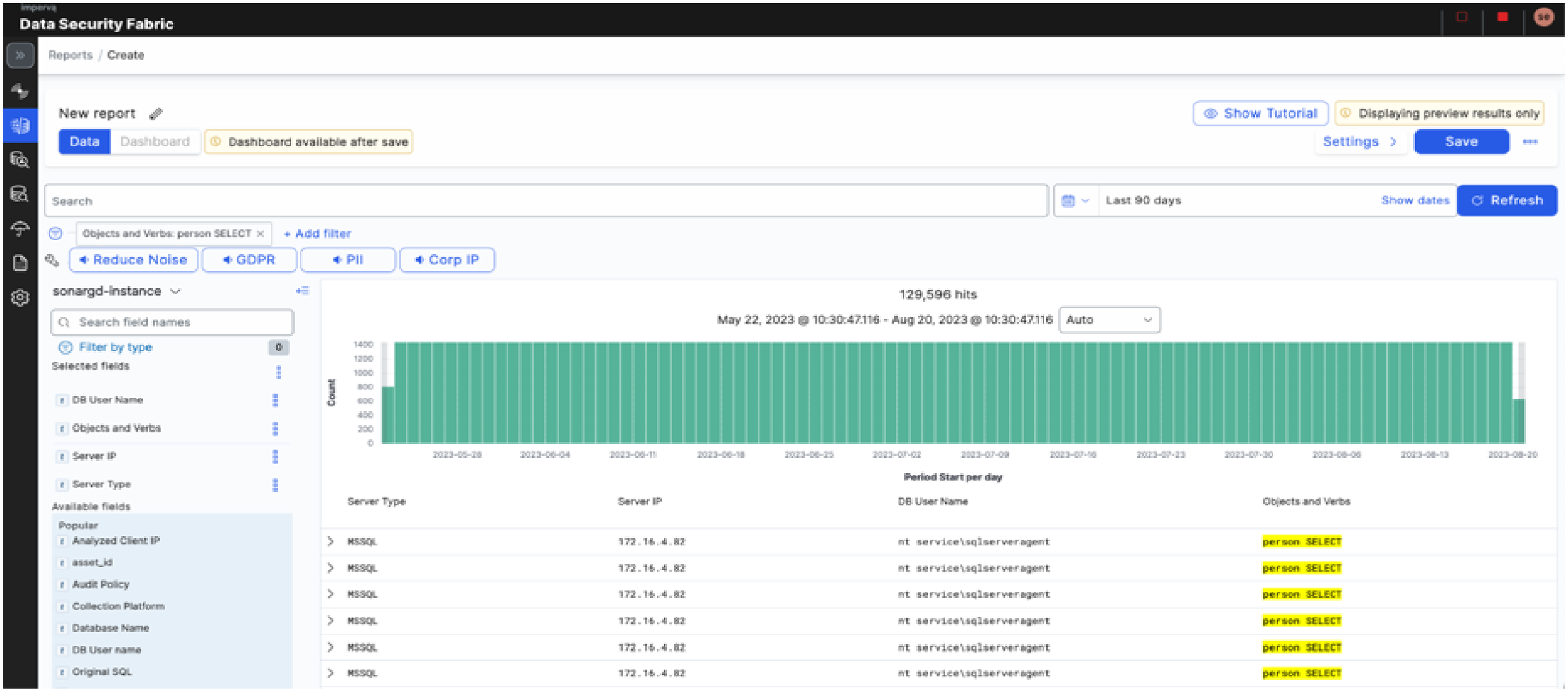
Elastyczne raportowanie



Przykład budowy raportu



Przykład budowy raportu



CryptoPanel

podsumowanie

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

Coś na wynos…

1. https://www.imperva.com/products/plans/

2. Data Secure Plan

a) Data Secure Base Plan (includes 8 servers), Annual Enhanced Subscription **USD 96390**

b) Add 92 to 491 servers to Data Secure Base Plan (per server), Annual Enhanced Subscription **USD 6237**

3. Rozwinięciem Data Secure jest Data 360.

a) Data 360 Base Plan (includes 8 servers), Annual Enhanced Subscription **USD 125307**

b) Add 1 to 6 servers to Data 360 Base Plan (per server), Annual Enhanced Subscription **USD 11794**

CryptoPanel

pytania i odpowiedzi

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel

quiz z upominkami

THALES
Building a future we can all trust

imperva
a Thales company

CLICO

CryptoPanel