Trellix

AI and data

The Good, the Bad and the Ugly

Arjen Wark & Hemant Pandya

Solution Engineer

Two Speaker Intro

Arjen Wark

Solution Engineer BeNeLux

Hemant Pandya

Solution Engineer ME

Trellix

AI is here to stay (The Good)

Trellix

Many advantages for (corporate) security enrichments and advise:

Trellix WISE

Personal benefit:

Chat GPT, Gemini, CoPilot etc.

The threat of Generative AI

Benefits to Cybercriminals (The Bad)

- Proficiency Prerequisites
- Quality for Quantity
- Operational Workload
- Automated Social Engineering

THE CYBERTHREAT REPORT

November 2023

Insights Gleaned from a Global Network of Experts, Sensors, Telemetry, and Intelligence

Presented by Trellix ADVANCED RESEARCH CENTER

AI risks (The Ugly)

Incorrect data fed into AI

Personal data fed into AI

Company data fed into AI

A.I. TURNS THIS SINGLE BULLET POINT INTO A LONG EMAIL I CAN PRETEND I WROTE.
A.I. MAKES A SINGLE BULLET POINT OUT OF THIS LONG EMAIL I CAN PRETEND I READ.
TOM FISH BURNE
©marketoonist.com

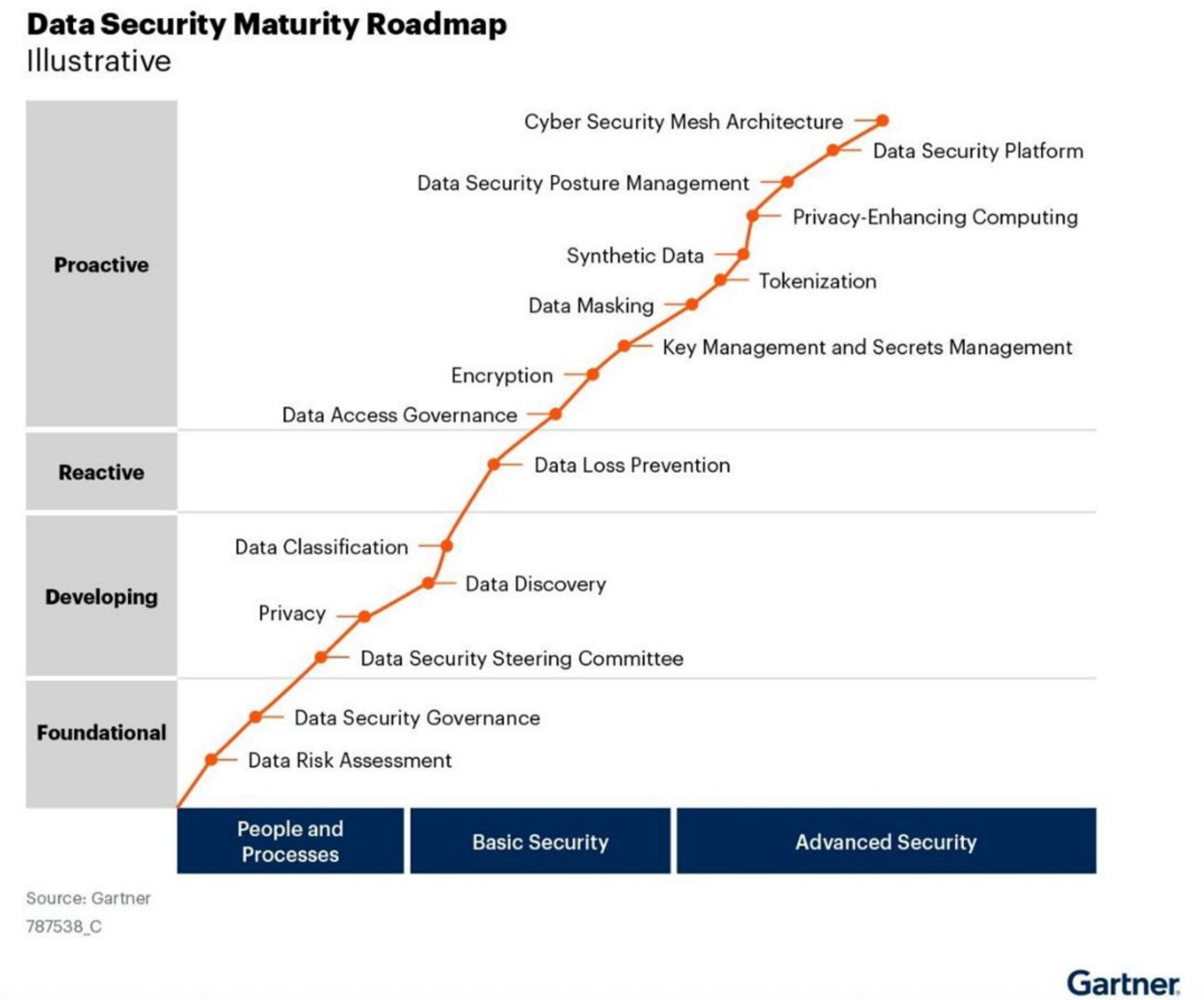
Trellix

Trellix DLP and AI

That is a WISE idea!

Align with Gartner's Data Security Roadmap

Protect the Data wherever it is



Data Security Maturity Roadmap

Illustrative

Source: Gartner

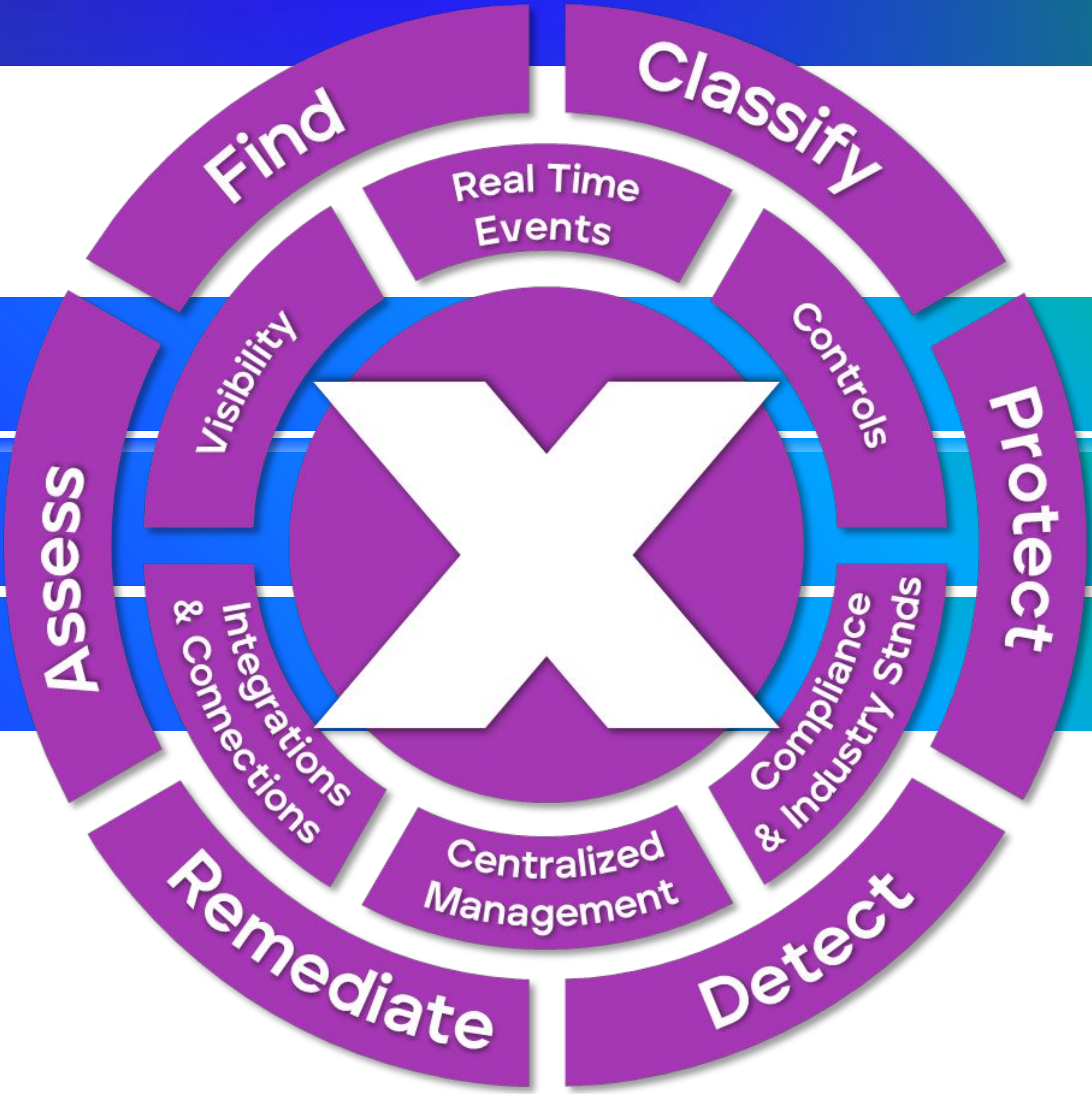
787538_C

Trellix Data Security

Trellix Data Loss Prevention

Trellix Data Encryption

Trellix Database Security



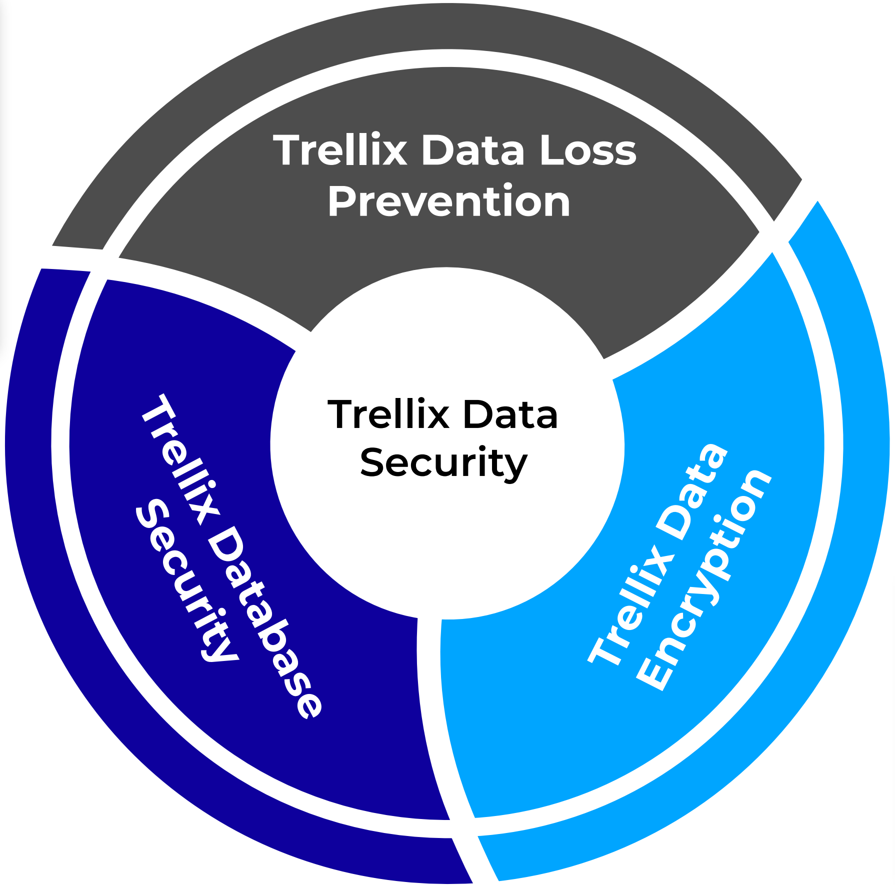
Trellix

Trellix Data Security

Protect the Data that Matters

Trellix Data Loss Prevention:
Safeguard against intentional and accidental data leaks

Trellix Data Classification:
Discover and Classify data wherever it is as it helps to protect your data



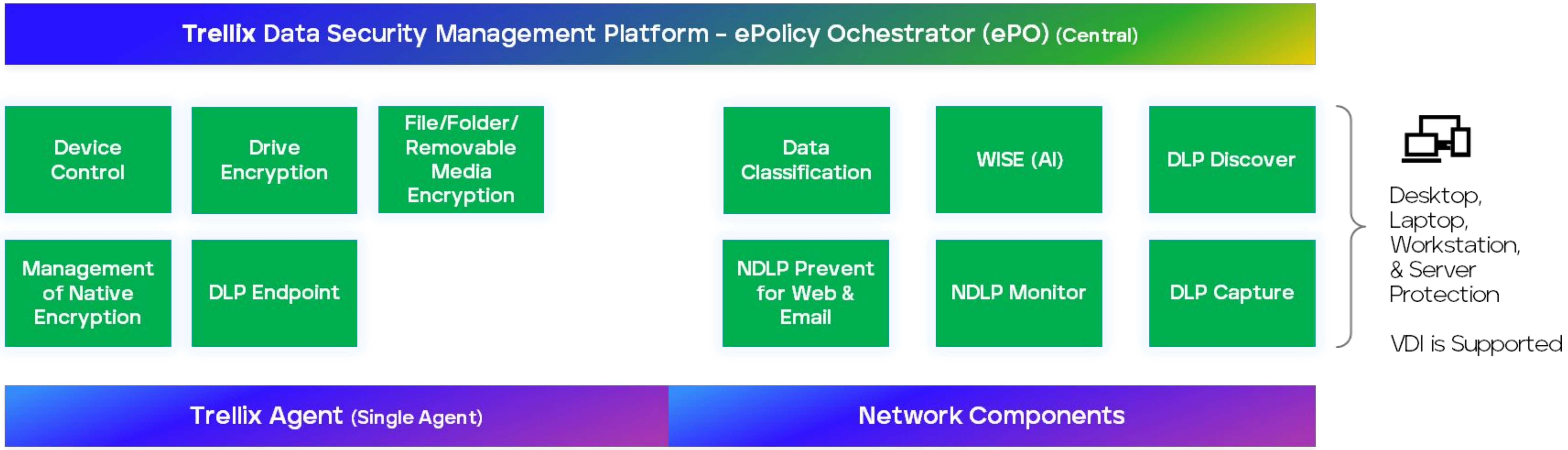
Trellix Database Security:
Find and defend databases and contained information

Trellix Data Encryption:
Protect enterprise and removable device data

Trellix

Trellix Data Security

Protect the Data that Matters



Trellix Data Security Management Platform – ePolicy Ochestrator (ePO) (Central)

Device Control

Drive Encryption

File/Folder/ Removable Media Encryption

Management of Native Encryption

DLP Endpoint

Data Classification

WISE (AI)

DLP Discover

NDLP Prevent for Web & Email

NDLP Monitor

DLP Capture

Desktop, Laptop, Workstation, & Server Protection

VDI is Supported

Trellix Agent (Single Agent)

Network Components

Trellix WISE

AI to Enhance the good

DLP Event Analysis

Security Analyst Event Review

An analyst typically takes a few minutes to hours to investigate an event.

This has been one of the biggest challenges organizations have faced with Data Loss Prevention which can lead to frustration and potentially scaling back their DLP program when dealing with hundreds of events that need to be investigated daily.

Common Investigation Questions Asked

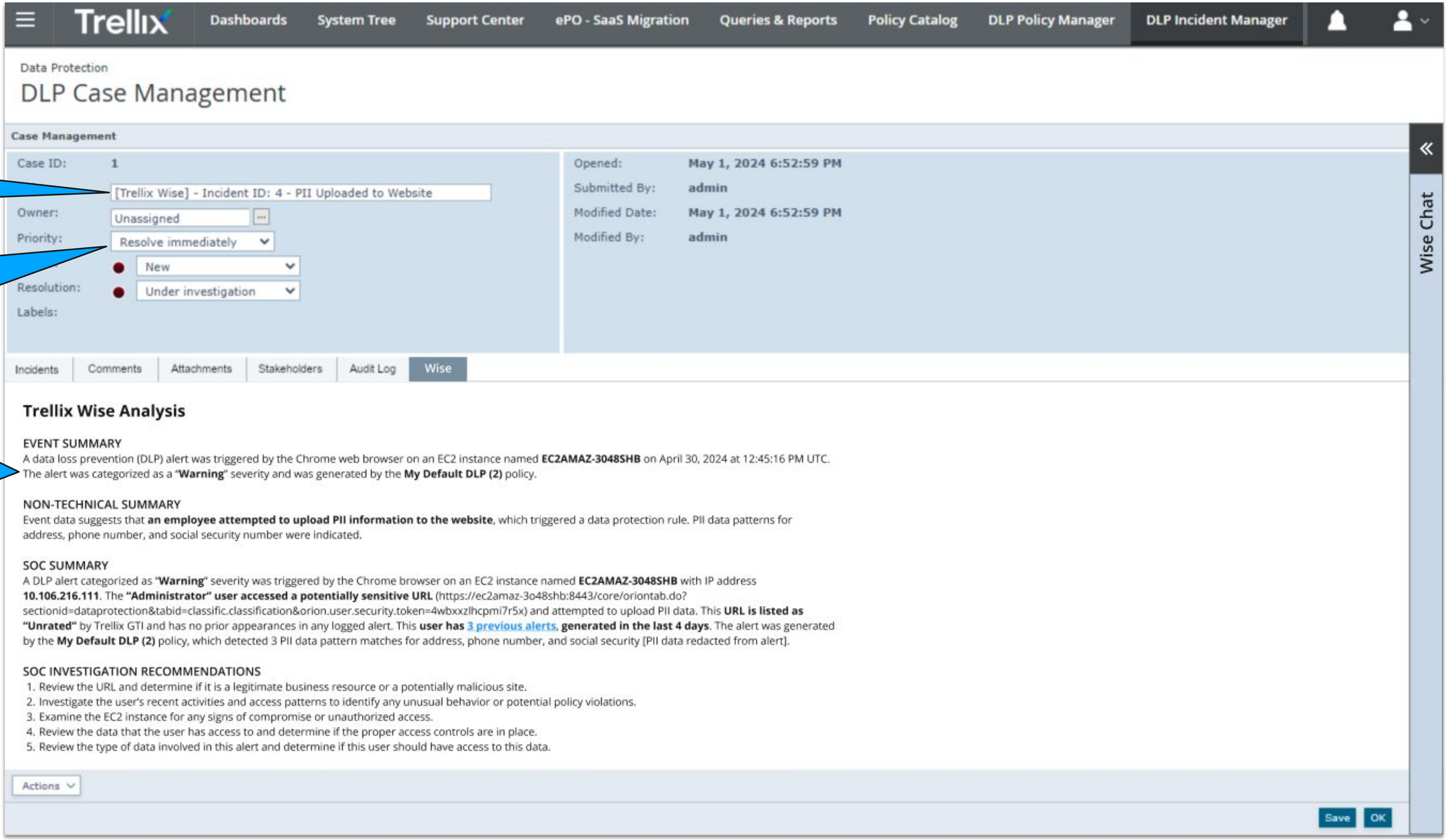
- Which events should I focus on investigating?
- What occurred with this event?
- How confident am I that this event should be investigated?
- How can I summarize what occurred the end-user who is not technical?
- What next steps should be taken to investigate this incident?
- Are there any changes that should be made to the rule that triggered?

Trellix Wise + DLP

Trellix Wise Analyzed Cases Annotated

Trellix Wise determines that the overall severity of the event should be raised bringing it to the attention of an analyst

Event Summary, Non-Technical Summary and Steps, SOC Summary and Steps all generated by Trellix Wise reducing the burden on an analyst



Data Protection

DLP Case Management

Case Management

Case ID: 1

[Trellix Wise] - Incident ID: 4 - PII Uploaded to Website

Owner: Unassigned

Priority: Resolve immediately

● New

Resolution: ● Under investigation

Labels:

Opened: **May 1, 2024 6:52:59 PM**

Submitted By: **admin**

Modified Date: **May 1, 2024 6:52:59 PM**

Modified By: **admin**

Trellix Wise Analysis

EVENT SUMMARY

A data loss prevention (DLP) alert was triggered by the Chrome web browser on an EC2 instance named **EC2AMAZ-3048SHB** on April 30, 2024 at 12:45:16 PM UTC. The alert was categorized as a "**Warning**" severity and was generated by the **My Default DLP (2)** policy.

NON-TECHNICAL SUMMARY

Event data suggests that **an employee attempted to upload PII information to the website**, which triggered a data protection rule. PII data patterns for address, phone number, and social security number were indicated.

SOC SUMMARY

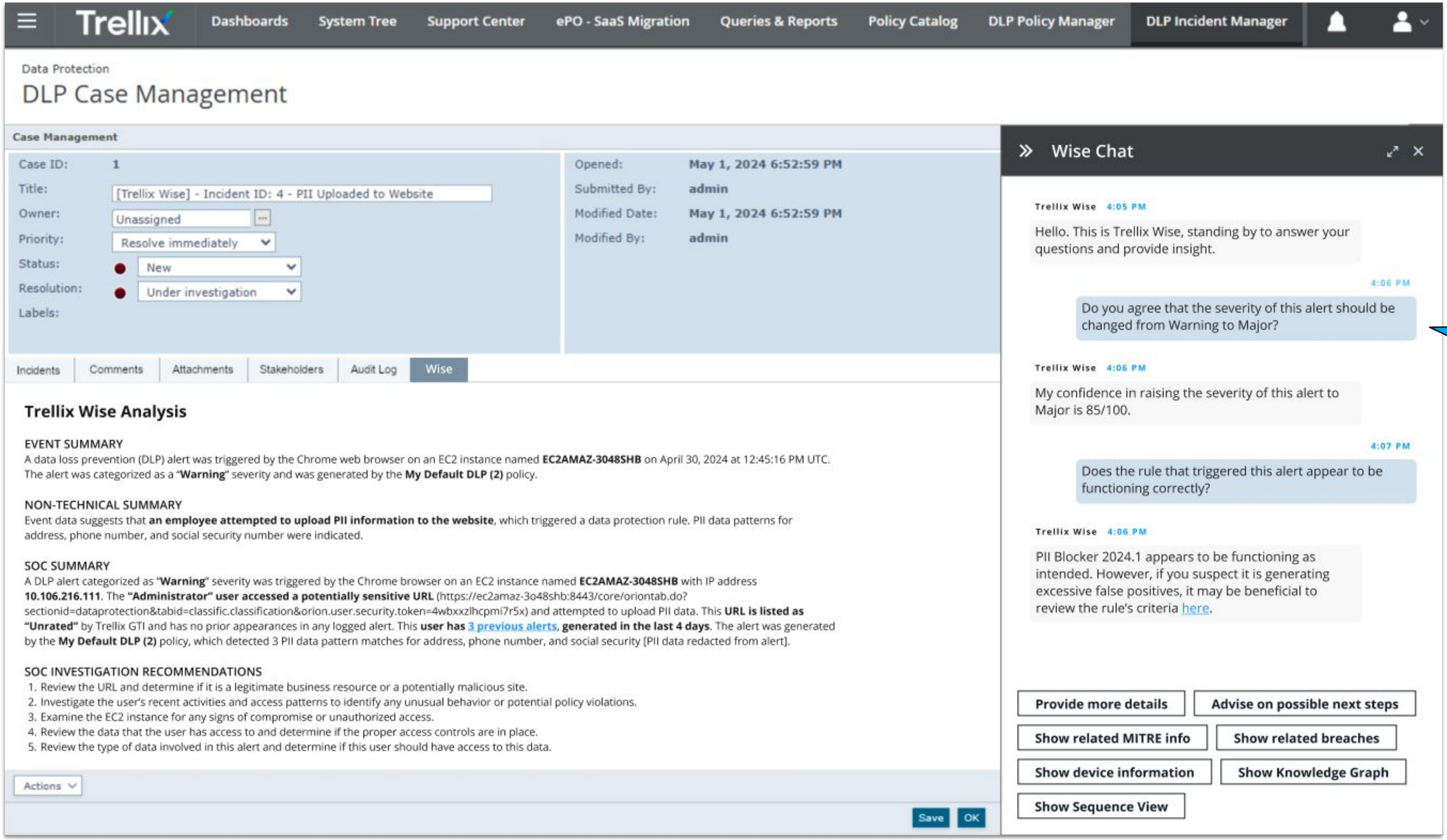
A DLP alert categorized as "**Warning**" severity was triggered by the Chrome browser on an EC2 instance named **EC2AMAZ-3048SHB** with IP address **10.106.216.111**. The **"Administrator" user accessed a potentially sensitive URL** (https://ec2amaz-3o48shb:8443/core/oriontab.do?sectionid=dataprotection&tabid=classific.classification&orion.user.security.token=4wbxxzlhcpmi7r5x) and attempted to upload PII data. This **URL is listed as "Unrated"** by Trellix GTI and has no prior appearances in any logged alert. This **user has** 3 previous alerts, **generated in the last 4 days**. The alert was generated by the **My Default DLP (2)** policy, which detected 3 PII data pattern matches for address, phone number, and social security [PII data redacted from alert].

SOC INVESTIGATION RECOMMENDATIONS

1. Review the URL and determine if it is a legitimate business resource or a potentially malicious site.
2. Investigate the user's recent activities and access patterns to identify any unusual behavior or potential policy violations.
3. Examine the EC2 instance for any signs of compromise or unauthorized access.
4. Review the data that the user has access to and determine if the proper access controls are in place.
5. Review the type of data involved in this alert and determine if this user should have access to this data.

Trellix

Trellix Wise + DLP



Data Protection

DLP Case Management

Case Management

Case ID:	1	Opened:	May 1, 2024 6:52:59 PM
Title:	[Trellix Wise] - Incident ID: 4 - PII Uploaded to Website	Submitted By:	admin
Owner:	Unassigned	Modified Date:	May 1, 2024 6:52:59 PM
Priority:	Resolve immediately	Modified By:	admin
Status:	● New		
Resolution:	● Under investigation		
Labels:			

Trellix Wise Analysis

EVENT SUMMARY
A data loss prevention (DLP) alert was triggered by the Chrome web browser on an EC2 instance named **EC2AMAZ-3048SHB** on April 30, 2024 at 12:45:16 PM UTC. The alert was categorized as a "**Warning**" severity and was generated by the **My Default DLP (2)** policy.

NON-TECHNICAL SUMMARY
Event data suggests that **an employee attempted to upload PII information to the website**, which triggered a data protection rule. PII data patterns for address, phone number, and social security number were indicated.

SOC SUMMARY
A DLP alert categorized as "**Warning**" severity was triggered by the Chrome browser on an EC2 instance named **EC2AMAZ-3048SHB** with IP address **10.106.216.111**. The **"Administrator" user accessed a potentially sensitive URL** (https://ec2amaz-3o48shb:8443/core/oriontab.do?sectionid=dataprotection&tabid=classific.classification&orion.user.security.token=4wbxxzlhcpmi7r5x) and attempted to upload PII data. This **URL is listed as "Unrated"** by Trellix GTI and has no prior appearances in any logged alert. This **user has 3 previous alerts, generated in the last 4 days**. The alert was generated by the **My Default DLP (2)** policy, which detected 3 PII data pattern matches for address, phone number, and social security [PII data redacted from alert].

SOC INVESTIGATION RECOMMENDATIONS
1. Review the URL and determine if it is a legitimate business resource or a potentially malicious site.
2. Investigate the user's recent activities and access patterns to identify any unusual behavior or potential policy violations.
3. Examine the EC2 instance for any signs of compromise or unauthorized access.
4. Review the data that the user has access to and determine if the proper access controls are in place.
5. Review the type of data involved in this alert and determine if this user should have access to this data.

Wise Chat

Trellix Wise 4:05 PM
Hello. This is Trellix Wise, standing by to answer your questions and provide insight.

4:06 PM
Do you agree that the severity of this alert should be changed from Warning to Major?

Trellix Wise 4:06 PM
My confidence in raising the severity of this alert to Major is 85/100.

4:07 PM
Does the rule that triggered this alert appear to be functioning correctly?

Trellix Wise 4:06 PM
PII Blocker 2024.1 appears to be functioning as intended. However, if you suspect it is generating excessive false positives, it may be beneficial to review the rule's criteria here.

Chat directly with Trellix Wise for additional context and investigation steps

Trellix

Trellix DLP

Preventing the Ugly

Trellix Data Protection

Protecting sensitive data in the age of AI

20-Apr-2023

- **Andy Logan – Solutions Architect - Data Protection**

One more thing...

Trellix Database Security

Find and defend databases and the information they contain

Before

- Unprotected databases and sensitive information exposed
- Unrestricted user access
- Unpatched misconfigured databases
- Lack of compliance reporting

How We Help

- Databases and sensitive information discovered
- Authorized access only
- Scan, patch and secure databases quickly
- Speed and simplify compliance reporting

After

- Visibility across supported databases
- Sensitive data secure
- Meet compliance standards
- Data events monitored and addressed

Trellix

Trellix Database Security

Find and defend databases and the information they contain

ONE COMPREHENSIVE OFFERING!

Virtual Patching

- Protect databases from known and unknown vulnerabilities without downtime
- Stop intrusions and other exploits
- Get extra security when patches are no longer available for legacy or out of date applications

Trellix Database Security

Vulnerability Manager

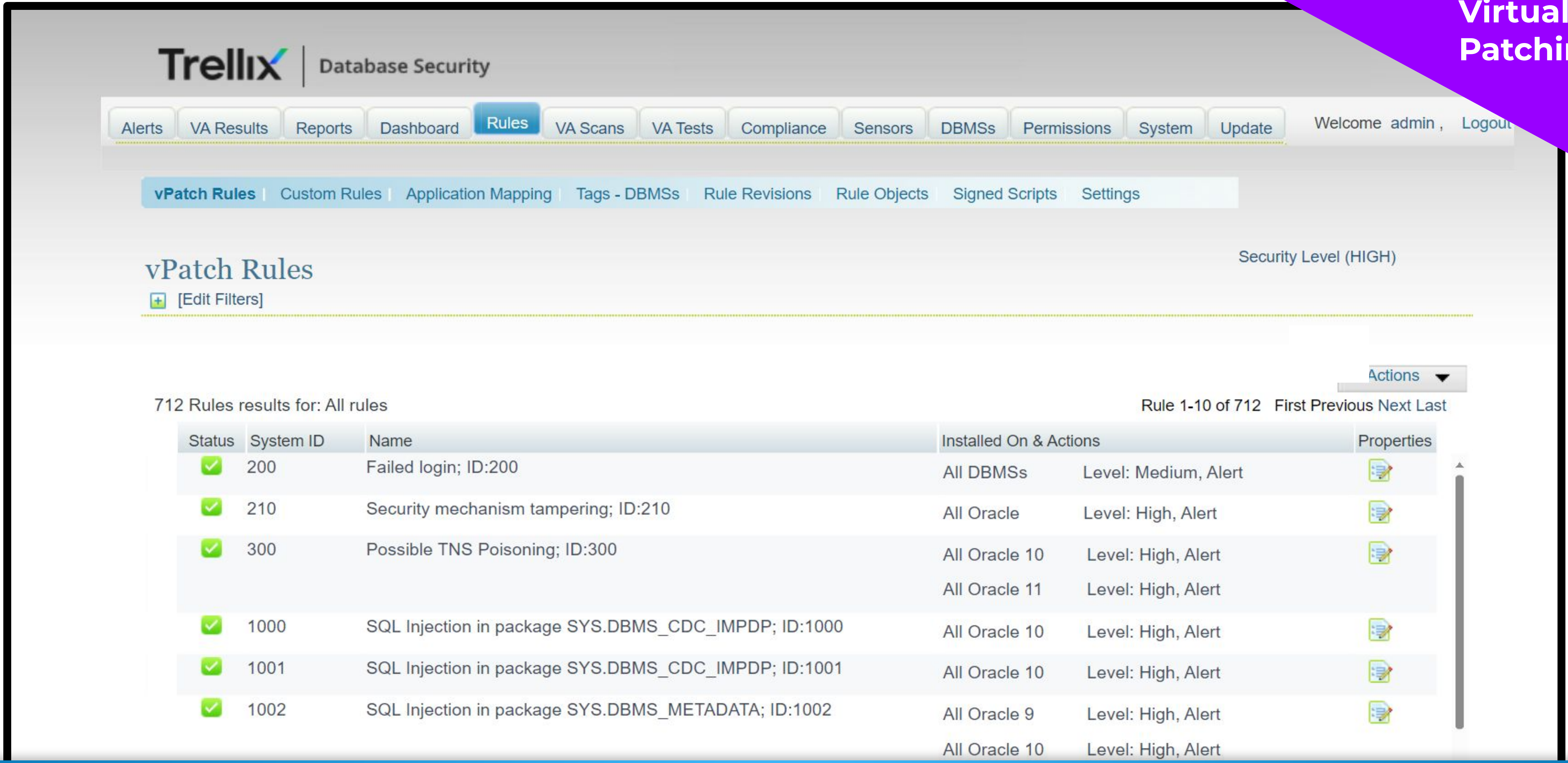
- Find databases and the sensitive information they contain through automated scanning
- Identify and prioritize vulnerabilities
- Get detailed remediation advice

Database Activity Monitoring

- Monitor, log, and control database access
- Identify and block potential threats before they can damage the environment
- Speed audit and compliance tasks

Expert professionals available for implementation and training. Centralized deployment, reporting, and tracking through a single management console available on-premises. Flexible licensing options.
Available as a stand-alone or added on to Data Security packages.

Virtual Patching



vPatch Rules

Security Level (HIGH)

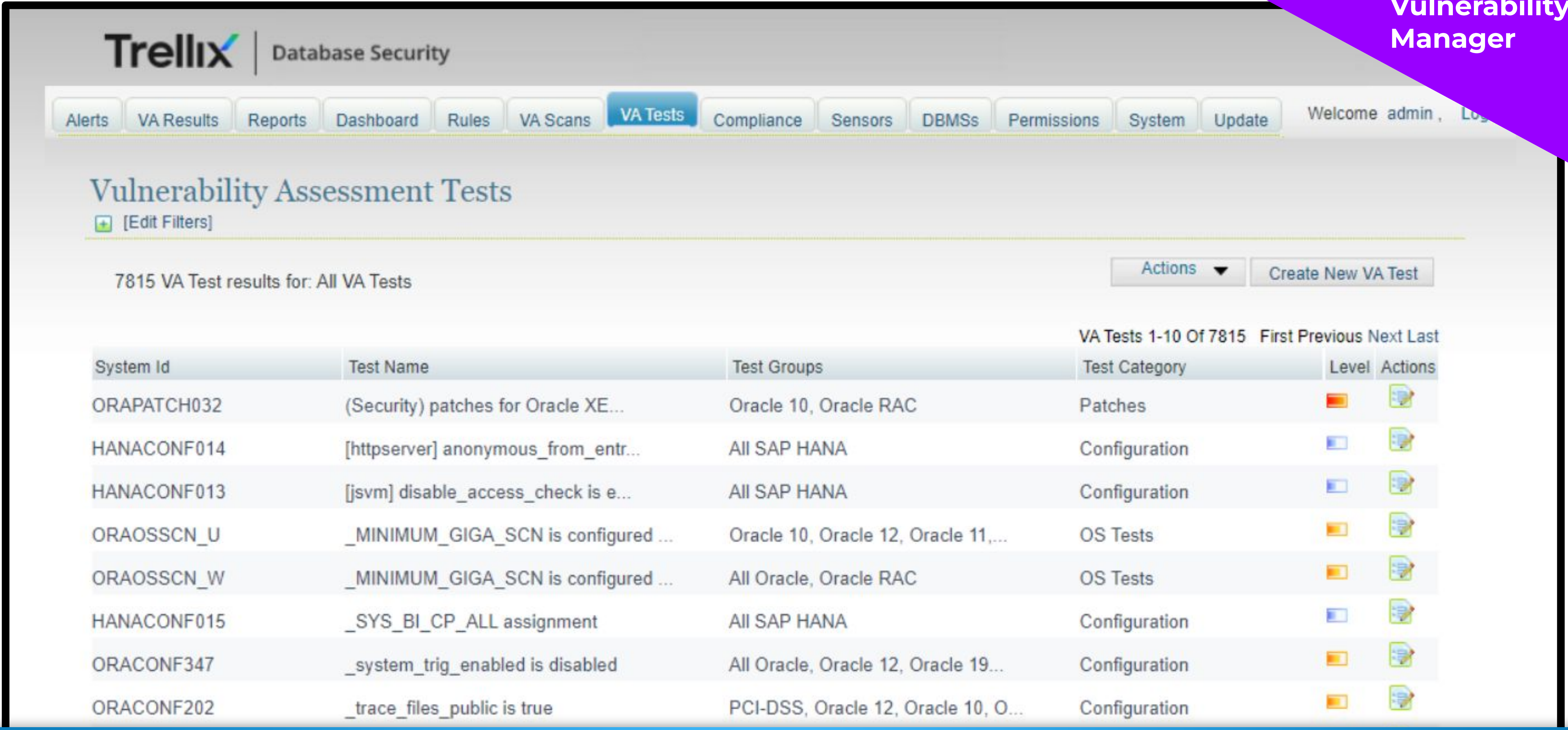
712 Rules results for: All rules

Rule 1-10 of 712

Status	System ID	Name	Installed On & Actions		Properties
✓	200	Failed login; ID:200	All DBMSs	Level: Medium, Alert	
✓	210	Security mechanism tampering; ID:210	All Oracle	Level: High, Alert	
✓	300	Possible TNS Poisoning; ID:300	All Oracle 10 All Oracle 11	Level: High, Alert Level: High, Alert	
✓	1000	SQL Injection in package SYS.DBMS_CDC_IMPDP; ID:1000	All Oracle 10	Level: High, Alert	
✓	1001	SQL Injection in package SYS.DBMS_CDC_IMPDP; ID:1001	All Oracle 10	Level: High, Alert	
✓	1002	SQL Injection in package SYS.DBMS_METADATA; ID:1002	All Oracle 9 All Oracle 10	Level: High, Alert Level: High, Alert	

vPatch Rules

Vulnerability
Manager



Vulnerability Assessment Tests

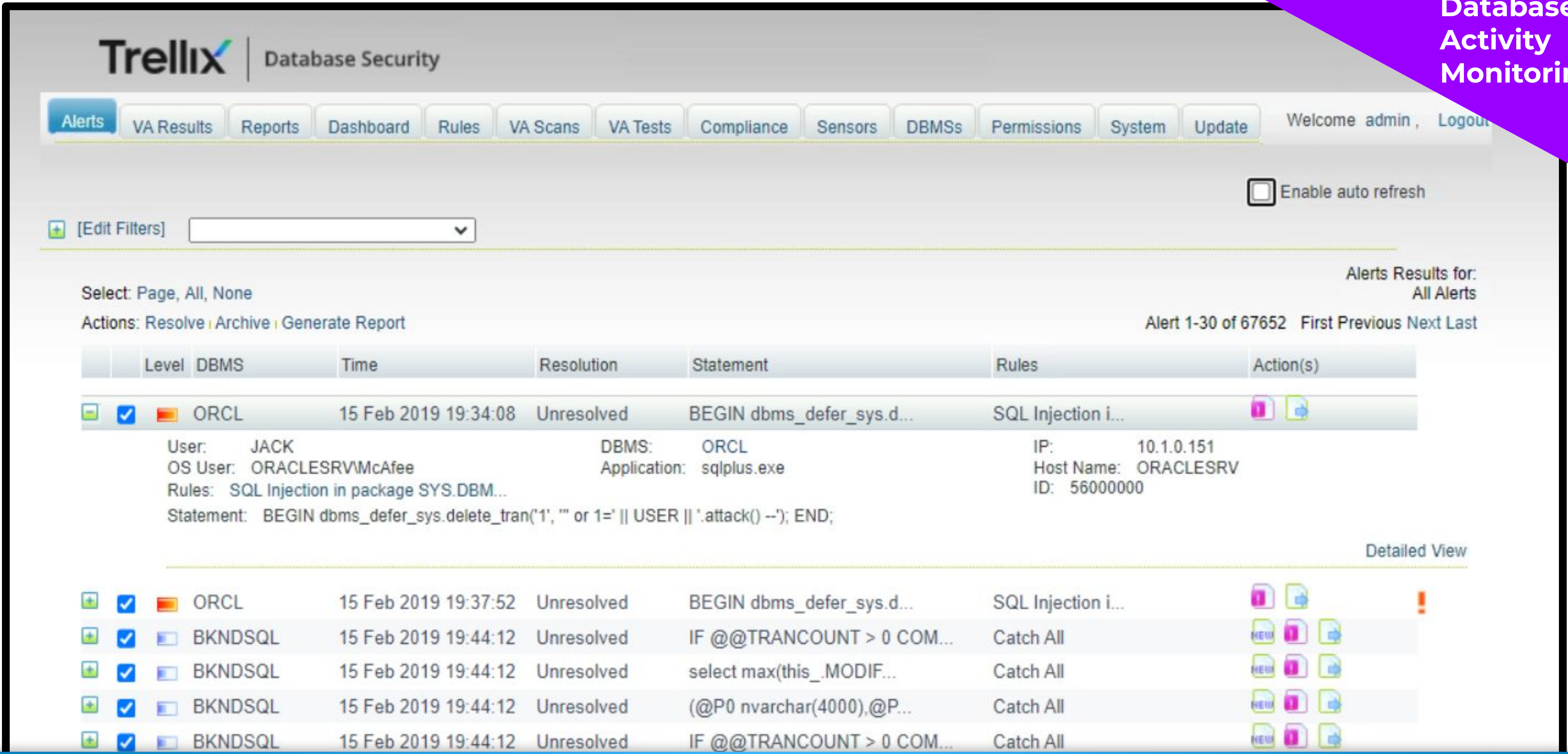
7815 VA Test results for: All VA Tests

VA Tests 1-10 Of 7815

System Id	Test Name	Test Groups	Test Category	Level	Actions
ORAPATCH032	(Security) patches for Oracle XE...	Oracle 10, Oracle RAC	Patches	🟥	✎
HANACONF014	[httpserver] anonymous_from_entr...	All SAP HANA	Configuration	🟦	✎
HANACONF013	[jsvm] disable_access_check is e...	All SAP HANA	Configuration	🟦	✎
ORAOSSCN_U	_MINIMUM_GIGA_SCN is configured ...	Oracle 10, Oracle 12, Oracle 11,...	OS Tests	🟧	✎
ORAOSSCN_W	_MINIMUM_GIGA_SCN is configured ...	All Oracle, Oracle RAC	OS Tests	🟧	✎
HANACONF015	_SYS_BI_CP_ALL assignment	All SAP HANA	Configuration	🟦	✎
ORACONF347	_system_trig_enabled is disabled	All Oracle, Oracle 12, Oracle 19...	Configuration	🟧	✎
ORACONF202	_trace_files_public is true	PCI-DSS, Oracle 12, Oracle 10, O...	Configuration	🟧	✎

Automated Vulnerability Scanning

Database Activity Monitoring



Select: Page, All, None

Actions: Resolve | Archive | Generate Report

Alerts Results for:
All Alerts

Alert 1-30 of 67652 First Previous Next Last

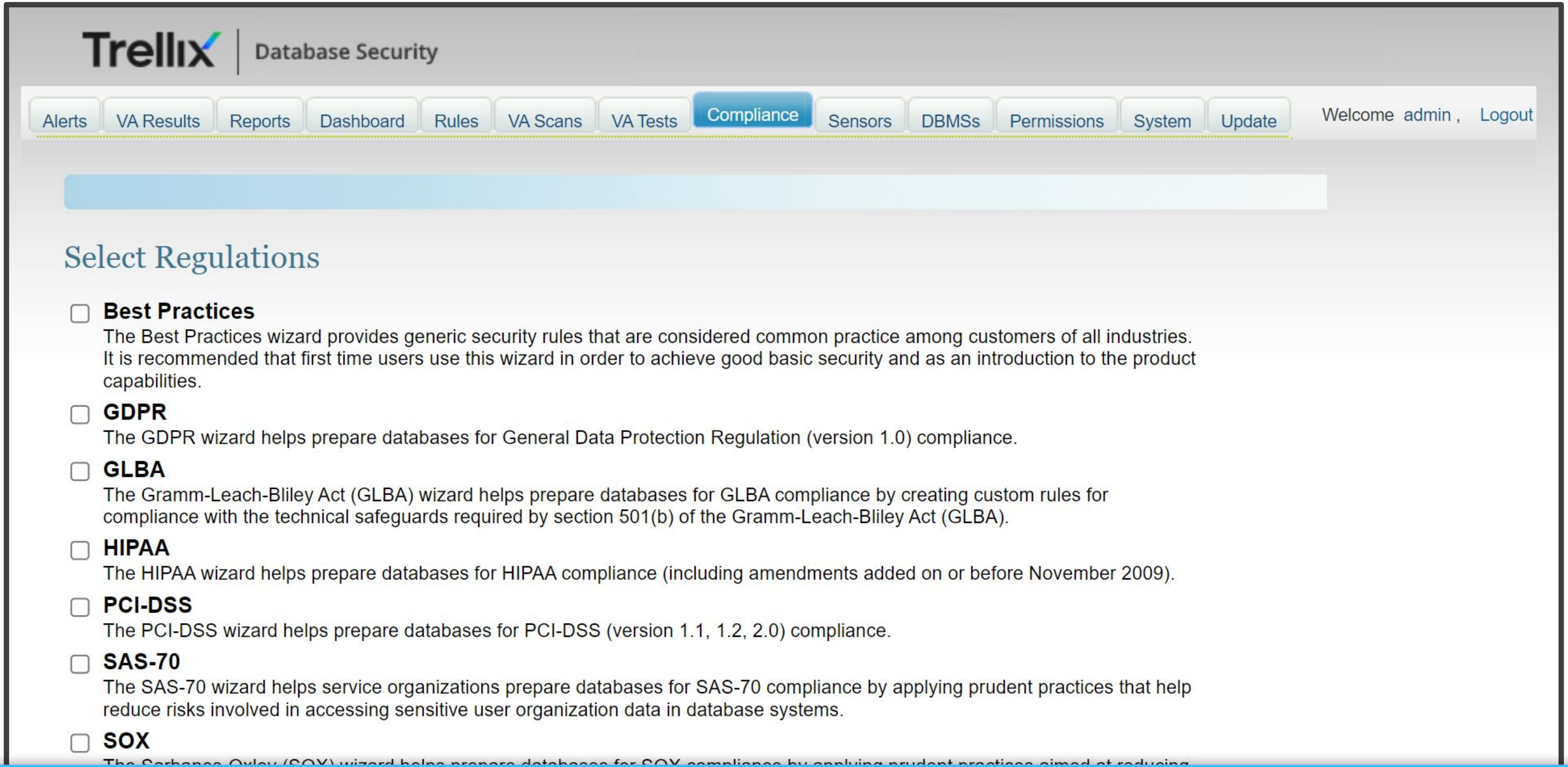
		Level	DBMS	Time	Resolution	Statement	Rules	Action(s)
⊟	☑	🟥	ORCL	15 Feb 2019 19:34:08	Unresolved	BEGIN dbms_defer_sys.d...	SQL Injection i...	

User: JACK
OS User: ORACLESRV\McAfee
Rules: SQL Injection in package SYS.DBM...
DBMS: ORCL
Application: sqlplus.exe
IP: 10.1.0.151
Host Name: ORACLESRV
ID: 56000000

Statement: BEGIN dbms_defer_sys.delete_tran('1', '" or 1=' || USER || '.attack() --'); END;

		Level	DBMS	Time	Resolution	Statement	Rules	Action(s)
⊞	☑	🟥	ORCL	15 Feb 2019 19:37:52	Unresolved	BEGIN dbms_defer_sys.d...	SQL Injection i...	!
⊞	☑		BKNDSQL	15 Feb 2019 19:44:12	Unresolved	IF @@TRANCOUNT > 0 COM...	Catch All	NEW
⊞	☑		BKNDSQL	15 Feb 2019 19:44:12	Unresolved	select max(this_.MODIF...	Catch All	NEW
⊞	☑		BKNDSQL	15 Feb 2019 19:44:12	Unresolved	(@P0 nvarchar(4000),@P...	Catch All	NEW
⊞	☑		BKNDSQL	15 Feb 2019 19:44:12	Unresolved	IF @@TRANCOUNT > 0 COM...	Catch All	NEW

Detailed Alerts and Notifications



Select Regulations

□ **Best Practices**
The Best Practices wizard provides generic security rules that are considered common practice among customers of all industries. It is recommended that first time users use this wizard in order to achieve good basic security and as an introduction to the product capabilities.

□ **GDPR**
The GDPR wizard helps prepare databases for General Data Protection Regulation (version 1.0) compliance.

□ **GLBA**
The Gramm-Leach-Bliley Act (GLBA) wizard helps prepare databases for GLBA compliance by creating custom rules for compliance with the technical safeguards required by section 501(b) of the Gramm-Leach-Bliley Act (GLBA).

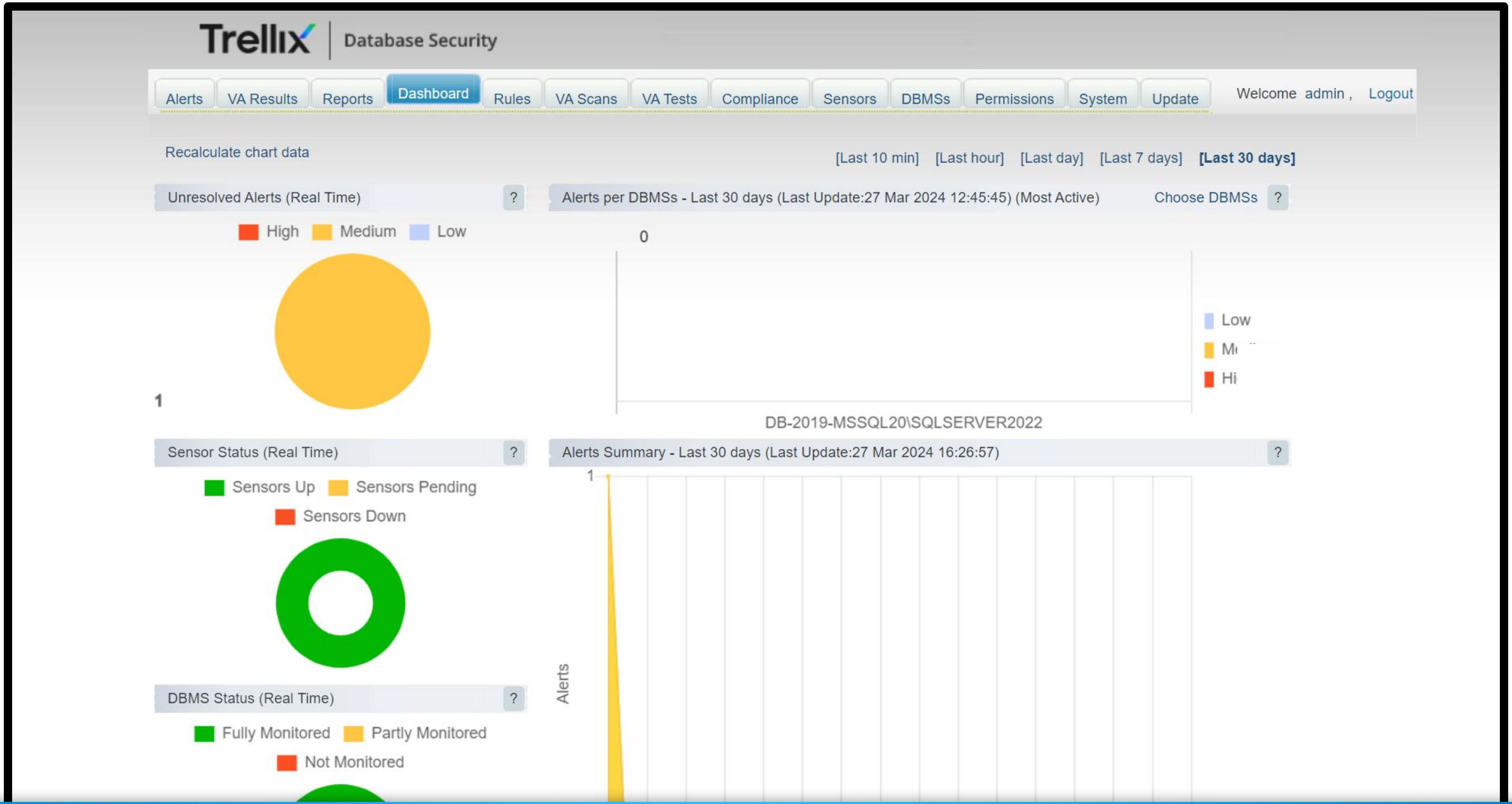
□ **HIPAA**
The HIPAA wizard helps prepare databases for HIPAA compliance (including amendments added on or before November 2009).

□ **PCI-DSS**
The PCI-DSS wizard helps prepare databases for PCI-DSS (version 1.1, 1.2, 2.0) compliance.

□ **SAS-70**
The SAS-70 wizard helps service organizations prepare databases for SAS-70 compliance by applying prudent practices that help reduce risks involved in accessing sensitive user organization data in database systems.

□ **SOX**
The Sarbanes-Oxley (SOX) wizard helps prepare databases for SOX compliance by applying prudent practices aimed at reducing

Regulatory & Audit Compliance


Trellix | Database Security
Alerts
VA Results
Reports
Dashboard
Rules
VA Scans
VA Tests
Compliance
Sensors
DBMSs
Permissions
System
Update
Welcome admin , Logout
Recalculate chart data
[Last 10 min] [Last hour] [Last day] [Last 7 days] [Last 30 days]
Unresolved Alerts (Real Time) ?
🟥 High 🟨 Medium 🟦 Low
1
Alerts per DBMSs - Last 30 days (Last Update:27 Mar 2024 12:45:45) (Most Active)
Choose DBMSs ?
0
Low
M
Hi
DB-2019-MSSQL20\SQLSERVER2022
Sensor Status (Real Time) ?
🟩 Sensors Up 🟨 Sensors Pending
🟥 Sensors Down
Alerts Summary - Last 30 days (Last Update:27 Mar 2024 16:26:57) ?
1
Alerts
DBMS Status (Real Time) ?
🟩 Fully Monitored 🟨 Partly Monitored
🟥 Not Monitored

Centralized Status and Events

Trellix