COMGUARD

cyber security masters

Trellix

Data Loss Prevention

Tomáš Koutný, Product Manager, COMGUARD a.s.
Thorsten Merz, Solutions Engineer, Trellix

19.09.2024

COMGUARD

Proč chránit data?

Krádeže a útoky na data v roce 2024

- Počet ukradených záznamů letos přesáhl miliardu
- AT&T komunikační společnost – ukradená data 73 milionů zákazníků
- Change Healthcare – ransomware ukradl data až 1/3 obyvatel USA pro účely vydírání
- Synnovis – krádež 300 milionů záznamů o pacientech (odložení operací + vydírání)
- Odcizení záznamů ze 165 firem, které používaly cloud od Snowflake
  - Stovky milionů záznamů z Ticketmaster
  - 79 milionů záznamů z Advanced Auto Parts
  - 30 milionů záznamů firmy TEG (softwarová společnost – sběr dat)

Cílem útočníků je ukrást Vaše data

Co kdyby jste měli řešení, které…

Chrání vaše data, ať jsou kdekoli a šifruje citlivá data

Chrání před vnitřními hrozbami

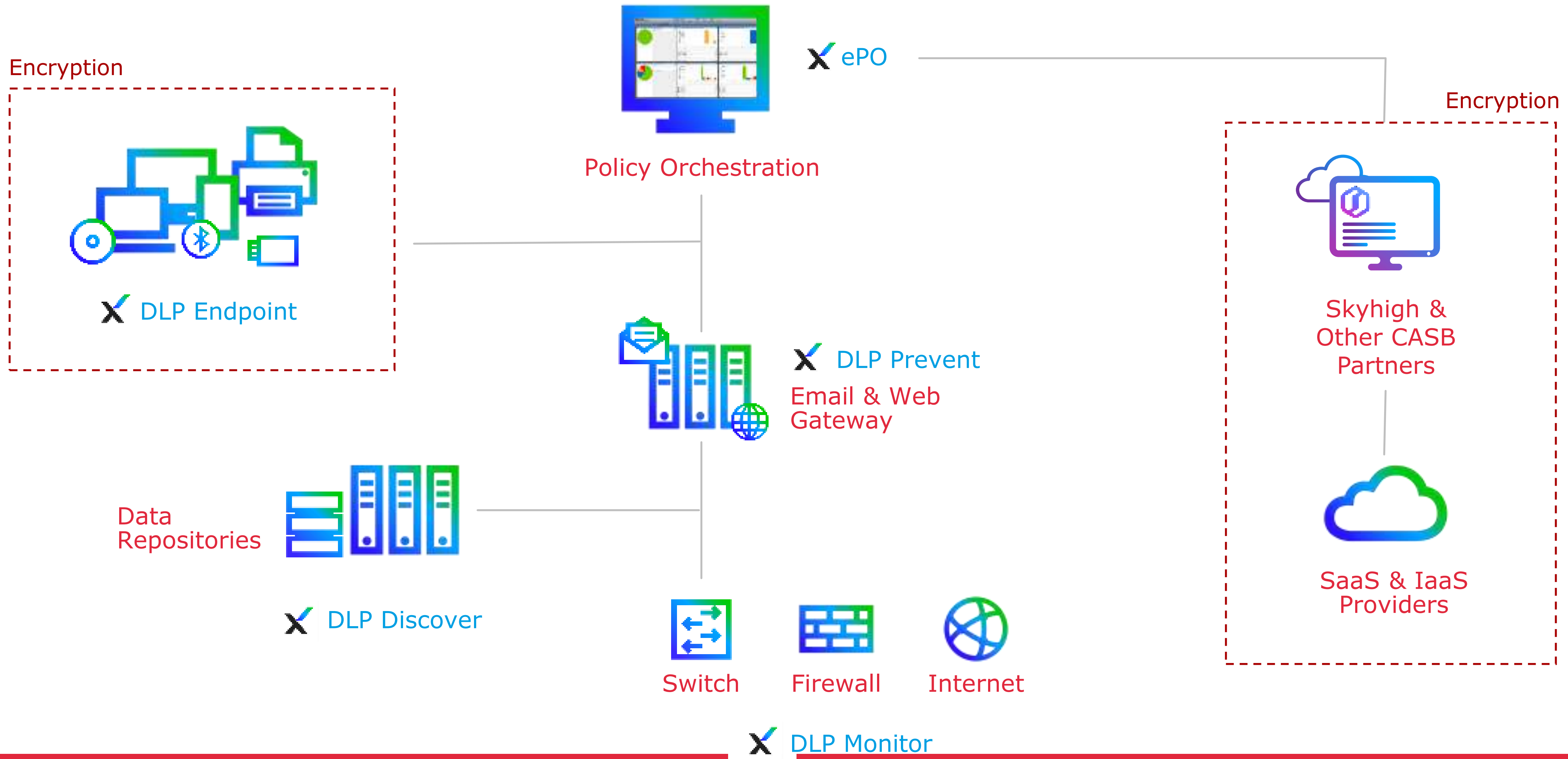
Zajišťuje soulad s předpisy

Trellix DLP

DLP – Data Loss Prevention

- Nástroj pro ochranu nejcennějšího majetku každé firmy
    - Klasifikace citlivosti dat - automatické i manuální
    - Centrální správa koncových bodů – Trellix ePolicy Orchestrator „ePO“
    - Prevence ztráty a zneužití dat – osobní nebo finanční data, patenty, zdrojové kódy,…
    - Průběžné reportování a monitorování v reálném čase
    - Jednotné nastavení politiky
    - Vysoká míra integrace s produkty třetích stran

Jak funguje Trellix Data Security?



Trellix

Trellix DLP and AI

That is a WISE idea!

Trellix

Trellix DLP and AI

That is a WISE idea!

Trellix

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

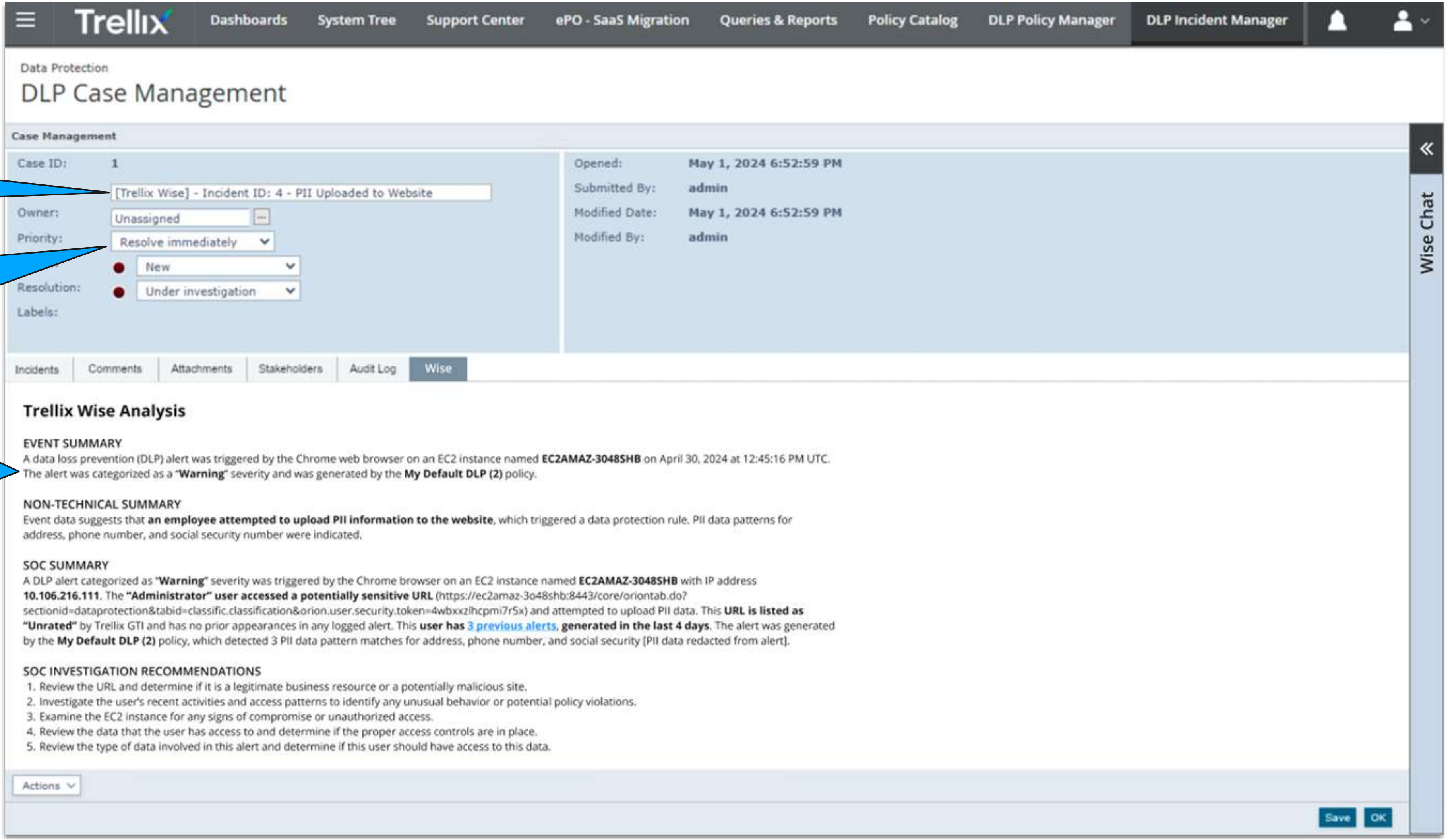
- Which events should I focus on investigating?
- What occurred with this event?
- How confident am I that this event should be investigated?
- How can I summarize what occurred the end-user who is not technical?
- What next steps should be taken to investigate this incident?
- Are there any changes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

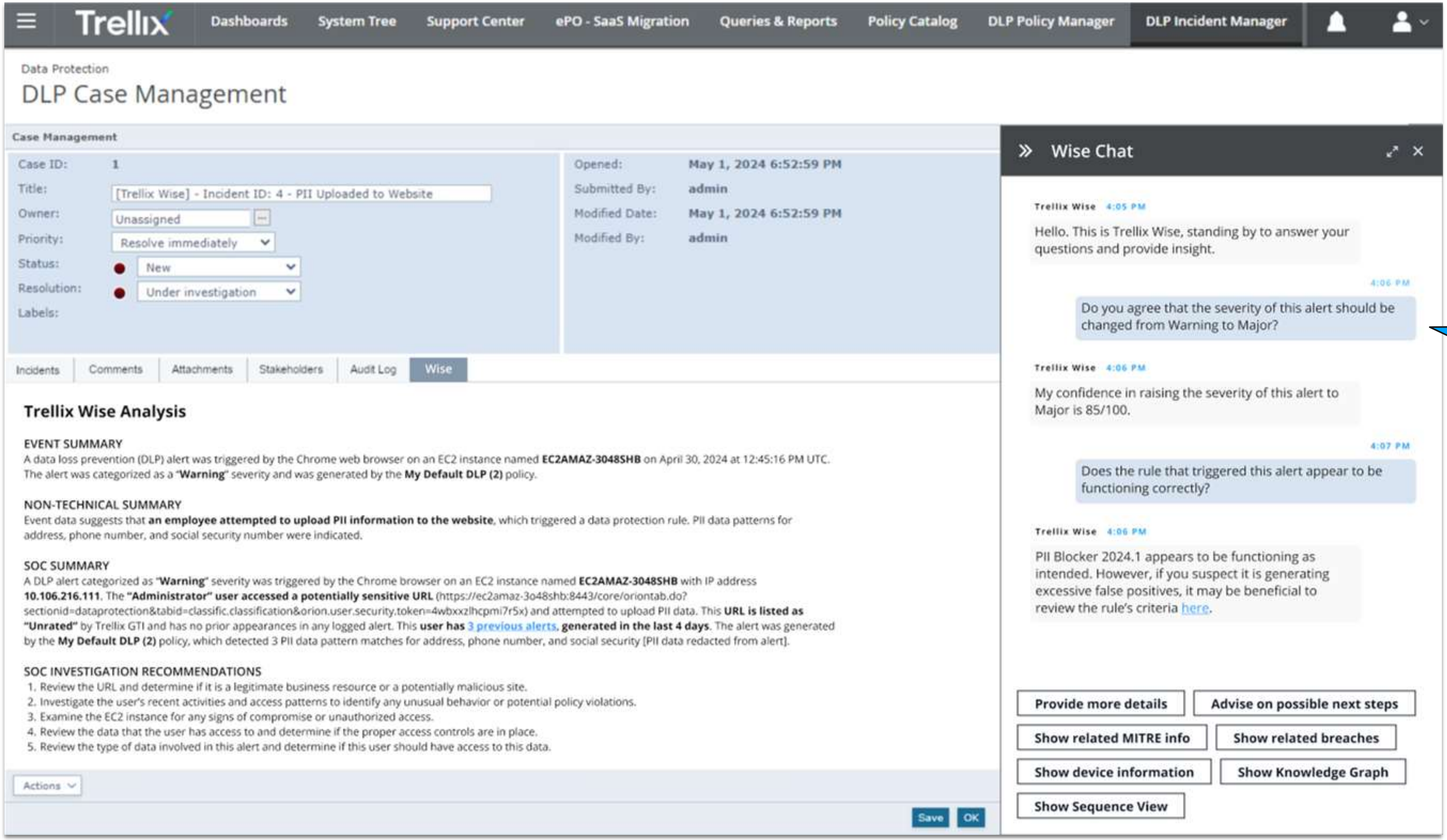
SOC SUMMARY

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 Wise + DLP



Data Protection

DLP Case Management

Case Management

Case ID:	1
Title:	[Trellix Wise] - Incident ID: 4 - PII Uploaded to Website
Owner:	Unassigned
Priority:	Resolve immediately
Status:	● 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.

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

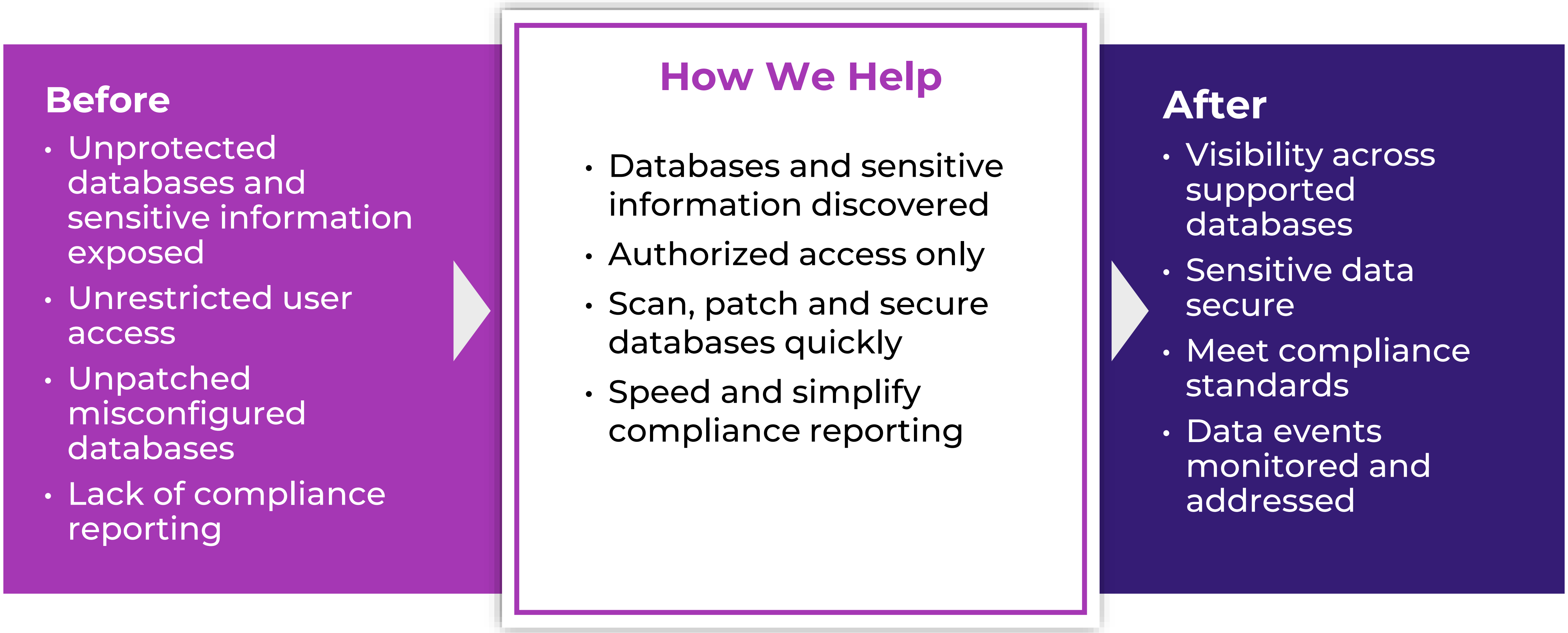
Preventing the Ugly

Trellix

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.

Trellix

COMGUARD

cyber security masters

Děkujeme za pozornost!