# CASE STUDY

Cyber Security Dashboard for a Global Oil Shipping Company

August, 2024
Authored By: Sumit Chimnani
Email: sumit.chimnani@ignatiuz.com

## Introduction

Maintaining strong cybersecurity is crucial in the global oil shipping sector to protect essential operations and secure sensitive data. Our team developed a comprehensive Cyber Security Dashboard for one of the global oil shipping companies worldwide. This advanced solution integrates various security data sources into a unified platform, providing real-time insights and enhancing the company's ability to respond to cybersecurity threats effectively.

## Problem Statement

1. **Complex Security Environment:** The company was managing a complex network of cybersecurity tools and platforms, each providing different types of data. This fragmentation made it challenging to achieve a cohesive view of their security posture.
2. **Real-Time Threat Detection:** With the increasing sophistication of cyber threats, the company required a solution capable of detecting and responding to threats in real-time across their extensive digital infrastructure.
3. **Data Management and Reporting:** The task of maintaining and reporting data from numerous sources was inefficient and challenging. The fragmented data sets made it hard to produce accurate reports and to get a clear view of the security situation.
4. **Compliance and Reporting:** The company needed to ensure compliance with industry regulations and standards while simplifying reporting processes for internal stakeholders and regulatory bodies.
5. **Incident Response Efficiency:** There was a need for a more efficient incident response mechanism to minimize potential damage and operational disruption from security incidents.

# List of Data Sources

To address the problem, the following data sources were utilized in the final version of the report, rest were eliminated.

### Taegis XDR
Extended Detection and Response for comprehensive threat detection and analytics.

### Qualys
Vulnerability management and security assessment to identify and address vulnerabilities.

### Mimecast
Email security and protection to guard against phishing and email-based threats.

### Backup SharePoint Repository
Backup and recovery status to ensure data integrity and availability.

### KnowBe4
Security awareness training and simulation to educate employees on cyber threats.

### Duo Admin Portal
Multi-factor authentication and access control to secure user access.

### Third Party Risk
Assessment of risks from third-party vendors to manage external security threats.

### Cloud Security Posture
Monitoring and managing cloud security configurations to maintain compliance and security.

### Cortex XDR
Advanced threat detection and response for comprehensive endpoint and network protection.

### Panorama Network Security
Network security management and monitoring for threat detection and prevention.

### CrowdStrike
Endpoint protection and threat intelligence to detect and respond to endpoint threats.

### Azure Sentinel
Cloud-native SIEM for intelligent security analytics and incident response.

### Splunk
Log management and operational intelligence for in-depth analysis and monitoring.

### IBM QRadar
Security information and event management for centralized security intelligence.

### Tenable
Vulnerability scanning and management to identify and address potential vulnerabilities.

### Forcepoint
Data security and threat protection to safeguard sensitive information.

### Darktrace
AI-driven threat detection and response to identify and neutralize emerging threats.

### AWS CloudWatch
Monitoring for AWS services to ensure the security and performance of cloud-based applications.

### Google Chronicle
Security analytics platform for advanced threat detection and investigation.

### Sumo Logic
Cloud-native log management and analytics for real-time insights and operational intelligence.

### ZScaler
Cloud security and access management to protect internet access and enforce security policies.

# Solution Summary

The Cyber Security Dashboard was created to integrate data from the diverse range of security tools and platforms utilized by the top 10 global oil shipping company. This solution consolidates multiple data sources into a single, interactive interface, providing real-time monitoring, advanced threat detection, and efficient incident response capabilities. Key features include:

1. **Unified Interface**
   Combines data from various sources into a cohesive and interactive dashboard.

2. **Real-Time Alerts**
   Delivers immediate notifications of security events and incidents.

3. **Trend Analysis**
   Uses historical data to identify trends and potential emerging threats.

4. **Data Visualization**
   Integrated the Oracle database with Power BI to gather and visualize the data. Created an interactive dashboard featuring various types of visualizations, including graphs and cards, to present real-time information and analytics of the security environment.

5. **Customizable Reporting**
   Provides tailored reports to meet specific client needs and regulatory requirements.

# Benefits

1. **Enhanced Visibility:** The centralized dashboard offers a comprehensive view of the company's security posture, making it easier to identify and address potential threats

2. **Improved Threat Detection:** Real-time data integration and advanced analytics enable quicker identification and response to security incidents.

3. **Efficient Data Management:** Streamlined data aggregation and reporting processes reduce the complexity and inefficiency of managing multiple data sources.

4. **Streamlined Reporting:** Simplified reporting processes facilitate regulatory compliance and provide clear insights to stakeholders.

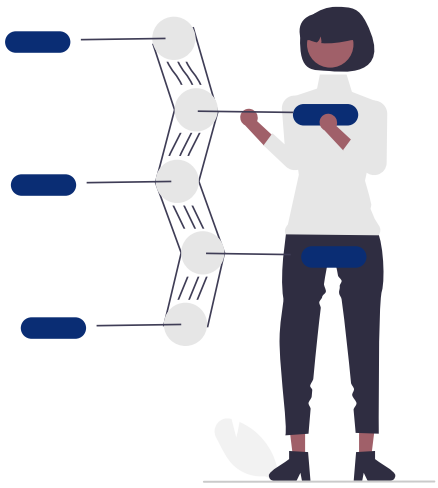
5. **Increased Efficiency:** Automation and integration reduce manual tasks, allowing security teams to focus on strategic actions.

6. **Proactive Security Management:** Actionable insights and trend analysis help anticipate and mitigate potential risks before they escalate.

7. **Scalability:** The solution is designed to grow with the company's needs, accommodating additional data sources and evolving security requirements.

# Conclusion

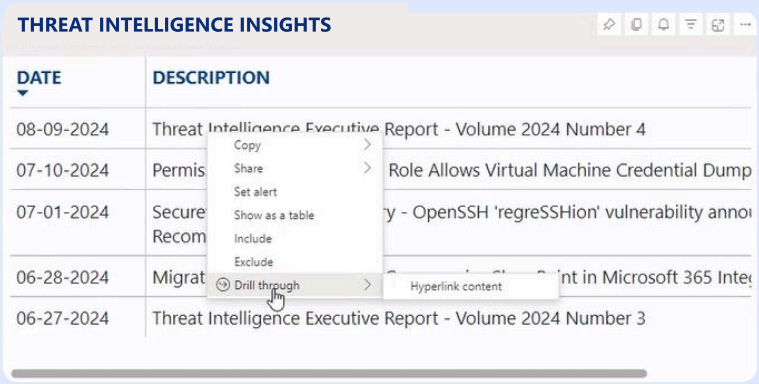
The Cyber Security Dashboard has significantly enhanced the cybersecurity capabilities of the global oil shipping company. By providing a unified view of their security landscape and integrating a wide range of data sources, the dashboard facilitates better threat management, improved reporting, and more efficient operations, ultimately strengthening the company's overall cybersecurity posture.



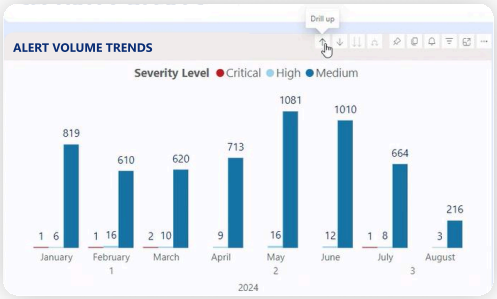
# Features and Functions of the Dashboard

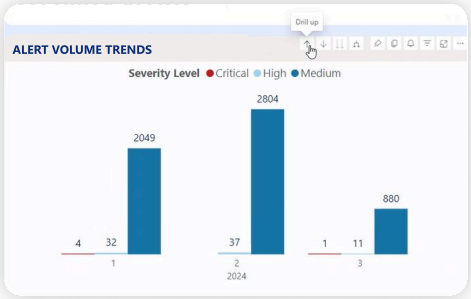
## Date Filtering


## Drill Through - Hyperlink



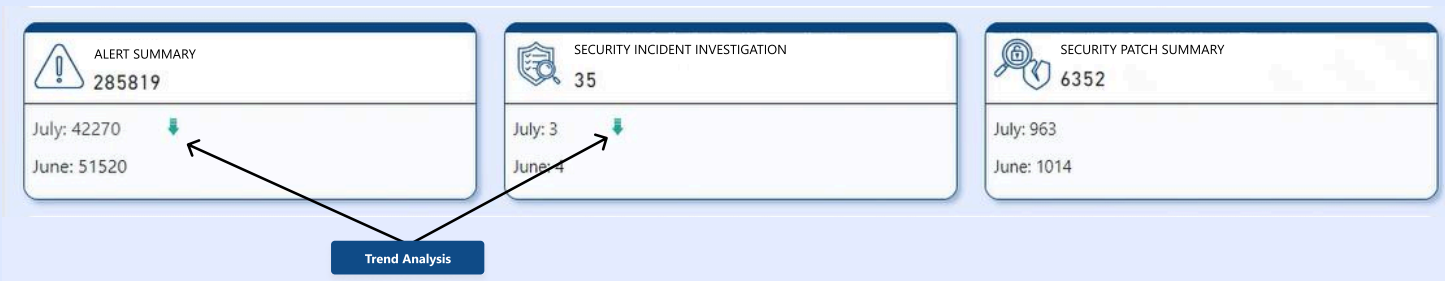

## Drill Up & Down



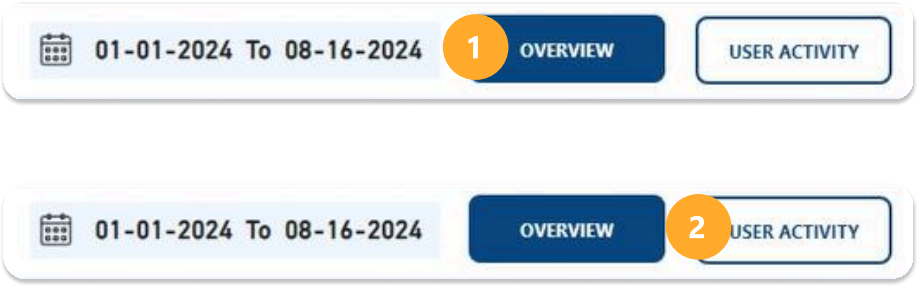





## Dynamic Cue Cards



# Navigation

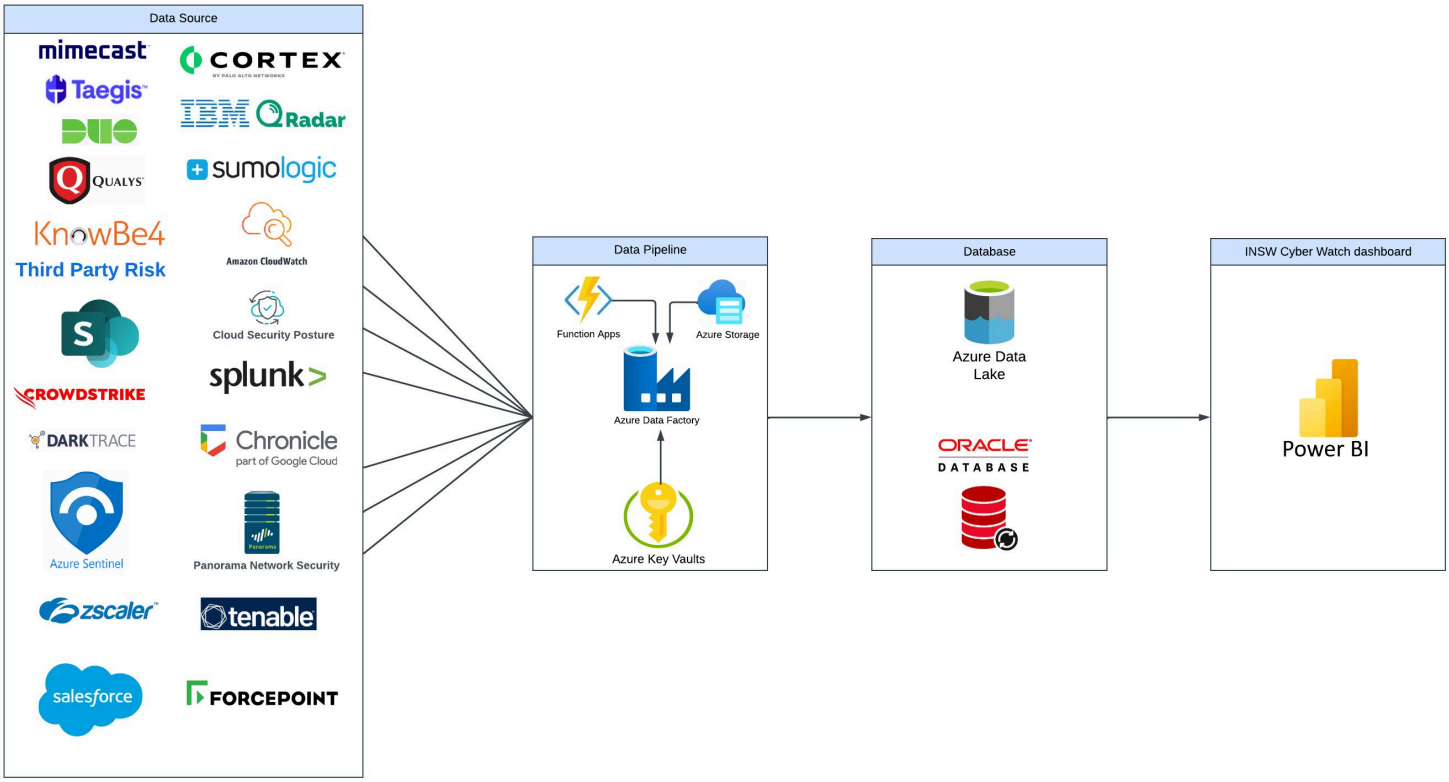



## Dynamic Formatting by Cell Value, Text, and Icons

**BACKUP STATUS**

| SERVICES | STATUS |
|---|---|
| Exchange Online | BACKLOGGED |
| Microsoft 365 Groups | BACKLOGGED |
| OneDrive for Business | BACKLOGGED |
| Project Online | BACKLOGGED |
| Public Folders | BACKLOGGED |
| SharePoint Online | BACKLOGGED |
| Teams | BACKLOGGED |

## Dashboard Based on Multiple Data Sets


Data Source
mimecast
CORTEX
Taegis
IBM QRadar
DUO
QUALYS
sumologic
KnowBe4
Third Party Risk
Amazon CloudWatch
Cloud Security Posture
splunk>
CROWDSTRIKE
DARKTRACE
Chronicle
part of Google Cloud
Azure Sentinel
Panorama Network Security
zscaler
tenable
salesforce
FORCEPOINT
Data Pipeline
Function Apps
Azure Storage
Azure Data Factory
Azure Key Vaults
Database
Azure Data Lake
ORACLE
DATABASE
INSW Cyber Watch dashboard
Power BI