Security Dashboard: Final Report

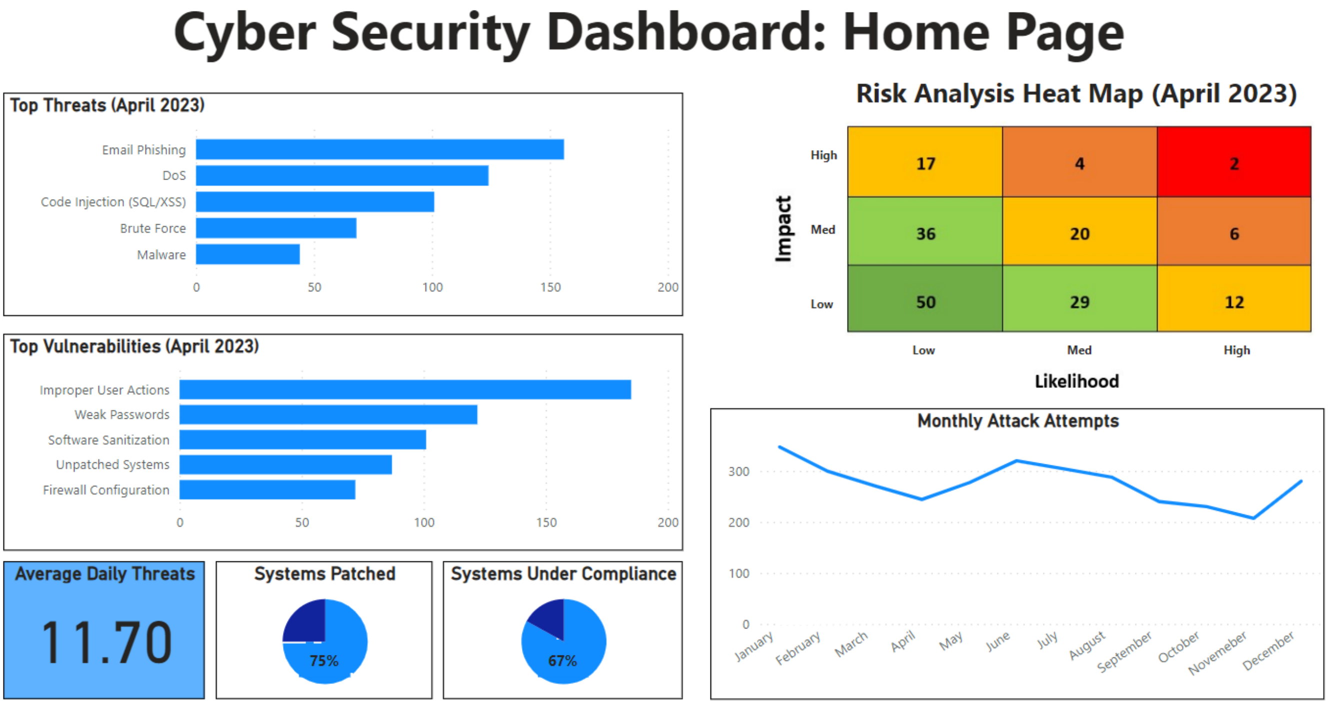
Harsh Bhakharia
University of North Florida
Jacksonville, Florida USA

Jonathan O’Berry
University of North Florida
Jacksonville, Florida USA

Andrew Simon
University of North Florida
Jacksonville, Florida US

Metric and Visualization Justification

Category: Home Page
ISO 27001 5.2 Policy
ISO 27001 6.1 Actions to Address Risks and Opportunities
ISO 27001 8.2/8.3 Information Security Risk Assessment/Treatment



Impact \ Likelihood	Low	Med	High
High	17	4	2
Med	36	20	6
Low	50	29	12

Metrics:

Top Threats/Vulnerabilities: These metrics were chosen to demonstrate which threat types are most common to our systems and which vulnerabilities these threats are trying to exploit. These two pieces of information help the organization prioritize its resources and best make an action plan for how to use those resources best. This goal aligns with the ISO 27001 6.1/83 standards, as they are used to plan actions to treat these threats. Additionally, a bar graph was chosen to clearly show the distance from one data point to the next, showing exactly how much more common/uncommon the event is.

Average Daily Threats: This KPI metric was chosen as a quick indicator for viewers of this report to see what the daily load of incoming threats looks like to the organization’s systems. As this type of report comes out monthly or quarterly, the necessary viewers can make decisions based on its fluctuation. This metric aligns with the ISO 27001 8.2 standard as it helps assess the average risk the organization faces daily.

Risk Heat Map: This metric visually represents the risk analysis process (impact + likelihood = risk) and how many risks the organization faces in the given month. The coloration of this visualization was chosen to match the heat map style most vulnerability scans use, indicating to the viewer that warmer colors are more severe and cooler colors are milder. This metric aligns with the ISO 27001 8.2 standard, providing information on the various severities of risks the organization faces.

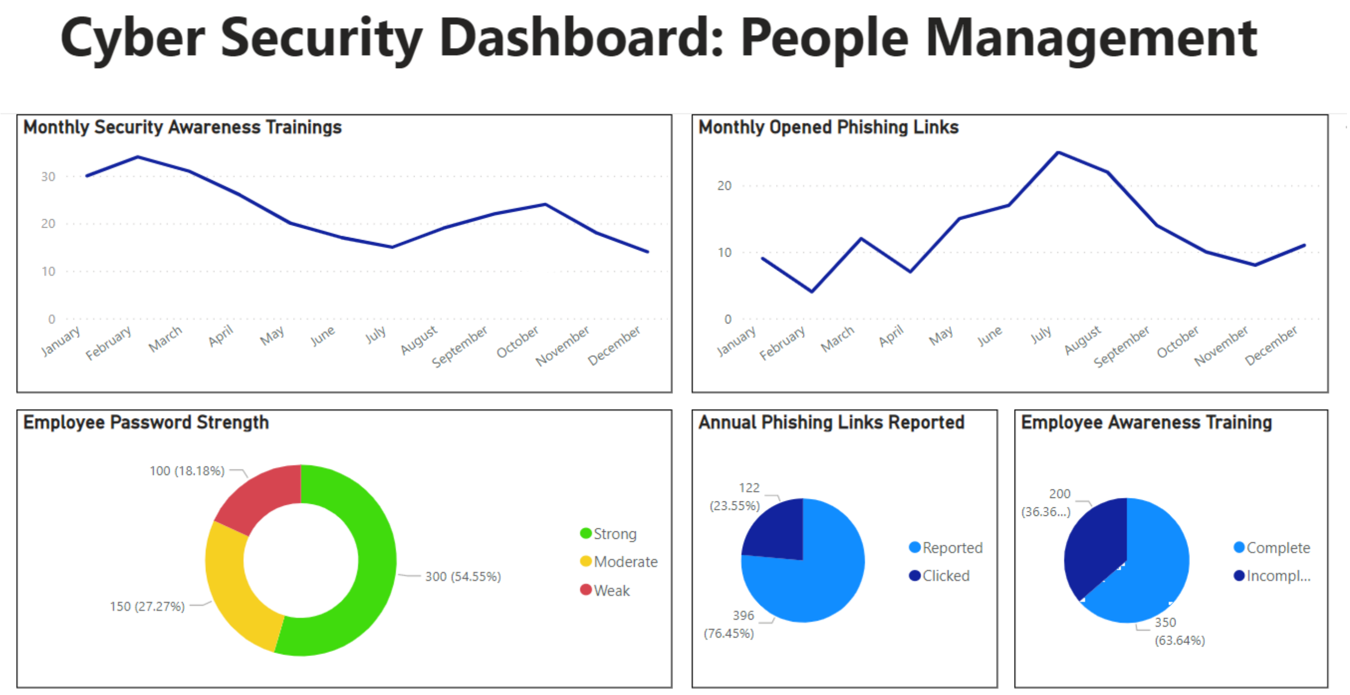
Systems Patched/Systems Under Compliance: The two KPI metrics quickly indicate to viewers how the organization's system applications are doing with their maintenance. Not having OS patched is one of the leading causes to impact, and having systems compliant with policy is crucial for audits. These metrics align with the ISO 27001 5.2 standard, delivering information about our systems being compliant with policy.

Monthly Attack Attempts: This metric tracks the volume of intrusion attempts over time. By monitoring the number of intrusion alerts, the organization can gain visibility into the frequency and trends of attempted intrusions. This information helps understand the threat level and effectiveness of existing security controls. It also assists in evaluating the organization's overall security posture and identifying areas that may require additional protection measures. This metric aligns with the ISO 27001 standard, specifically section 8.2 on Information Security Risk Assessment, which emphasizes the need for ongoing monitoring and assessment of risks.

Category: People Management

ISO 27002 7.2 Human Resource Security: During Employment

ISO 27001 7.2/7.3 Competence/Awareness



Metrics:

Percent of Employees with Finished Security Awareness Training: This metric is important as it provides insight into how well-trained our employees are in terms of security practices and procedures.

By measuring the percentage of employees who have completed security training, we can assess the overall effectiveness of our training programs and identify any gaps in employee knowledge or compliance. This metric aligns with the ISO 27002 standard, specifically section 7.2 on Human Resource Security: During Employment, which emphasizes the importance of providing appropriate training to employees.

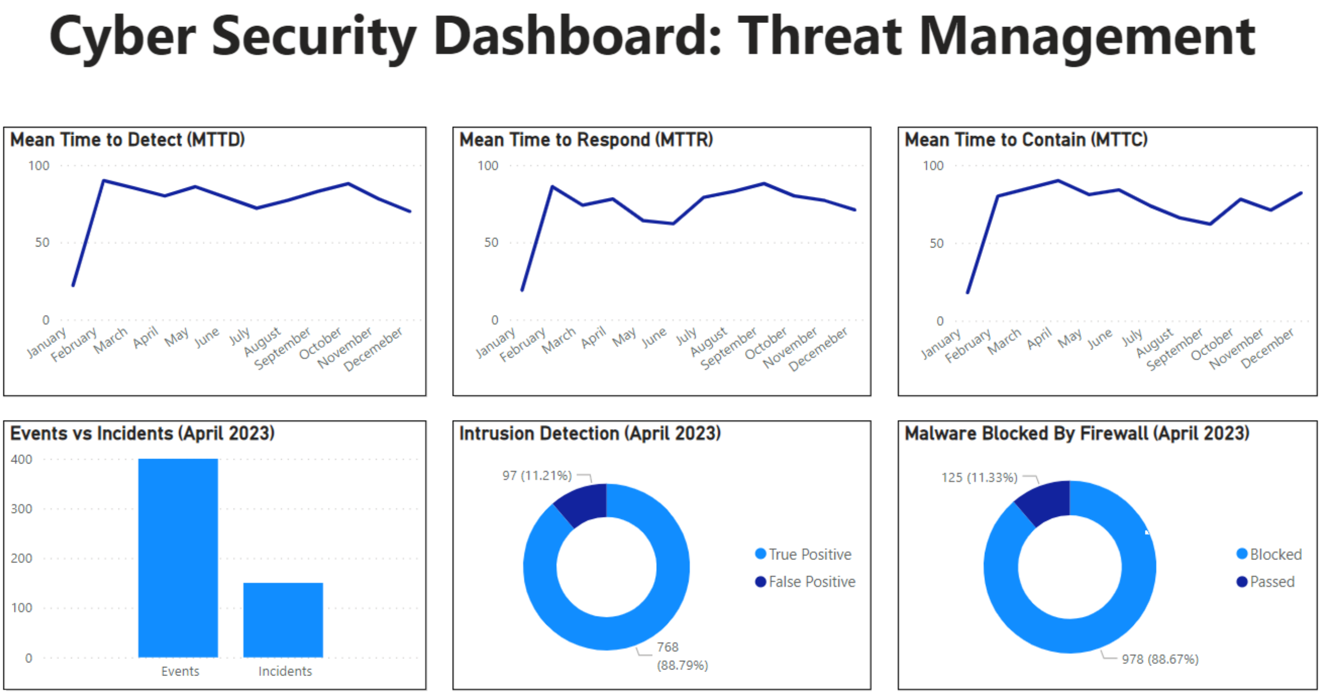
Monthly Security Awareness Training: This metric tracks the frequency of awareness trainings conducted within the organization. By measuring the number of awareness trainings over time, we can ensure that employees are regularly exposed to security awareness materials and reinforce good security practices. This metric aligns with the ISO 27002 standard, specifically section 7.2 on Human Resource Security: During Employment, which emphasizes the need for ongoing awareness programs.

Employee Password Strength: This metric measures the percentage of weak passwords in the employee database, indicating the vulnerability of user accounts to be compromised. By monitoring the strength of passwords used by employees, we can assess the effectiveness of security training and enforce password policies to mitigate the risk of unauthorized access. This metric aligns with the ISO 27002 standard, specifically section 7.2 on Human Resource Security: During Employment, which emphasizes the need to manage the use of passwords effectively. The visualization was chosen to show the percentage of the employee populations and how well their passwords were designed. The colors chosen aim to indicate to the viewer that green means good/secure, yellow means average/needs improvement, and red means bad/insecure.

Monthly Opened Phishing Links/Annual Phishing Links Reported: These two metrics measure the effectiveness of the organization’s awareness training and help paint a picture of how much of an impact employee user error has on the security of the organization’s systems. During employment (ISO 27002 7.2), it is important that the effect the awareness trainings on user actions is measured to better inform the necessary goals of future training steps. We chose to measure phishing events because they are a common vector involving human error and are a strong focus in many awareness trainings.

Category: Monitoring/Vulnerabilities

ISO 27002 12.2 Protection From Malware
ISO 27002 12.6 Technical Vulnerability Management
ISO 27002 16.1 Management of Information Security Incidents and Improvements



Cyber Security Dashboard: Threat Management

Metrics:

Mean time to detect (MTTD): This metric measures the average time it takes for the organization to detect intrusion or security incidents. By monitoring the MTTD, we can assess the effectiveness of our detection mechanisms and incident response processes. A shorter MTTD indicates a more efficient and proactive approach to identifying security threats, reducing the potential impact of security incidents. This metric aligns with ISO 27002 standard, specifically sections 12.2 on Protection from Malware and 16.1 on Management of Information Security Incidents and Improvements.

Mean time to respond (MTTR): This metric measures the average time it takes for the organization to respond and neutralize threats or security incidents once detected. By monitoring the MTTR, we can evaluate the effectiveness of our incident response procedures and the efficiency of our incident handling teams. A shorter MTTR indicates a more effective response to security incidents, minimizing potential damage and downtime. This metric aligns with ISO 27002 standard, specifically sections 12.2 on Protection from Malware and 16.1 on Management of Information Security Incidents and Improvements.

Mean time to contain (MTTC): This metric measures the average time it takes for the organization to contain and shut down all attack vectors once a security incident is detected. By monitoring the MTTC, we can assess the effectiveness of our containment procedures and the ability to minimize further impact. A shorter MTTC indicates a more efficient containment process, reducing the potential for data breaches or prolonged disruptions. This metric aligns with ISO 27002 standard, specifically sections 12.2 on Protection from Malware and 16.1 on Management of Information Security Incidents and Improvements.

Intrusion Detection (False Positives): This metric measures the percentage of false positives generated by the Intrusion Detection System (IDS). It helps assess the effectiveness and accuracy of the IDS in identifying and blocking actual security threats without excessive false alerts. A lower percentage of false positives indicates a more reliable IDS and reduces the operational burden of investigating and managing false alarms. This metric aligns with ISO 27002 standard, specifically section 12.6 on Technical Vulnerability Management.

Events vs. Incidents: This metric compares the number of attempted attacks against the number of actual security incidents. It helps evaluate the effectiveness of our security controls and the organization's ability to defend against attacks. A higher ratio of attempted attacks to incidents indicates that our controls effectively mitigate and prevent successful attacks. This metric aligns with ISO 27002 standard, specifically section 12.6 on Technical Vulnerability Management and 16.1 on Management of Information Security Incidents and Improvements. This visualization was chosen to demonstrate that all incidents are events. The viewer can use the bars in the graph to visually see the difference between the two, indicating how much or how little the tools are stopping events from becoming incidents.

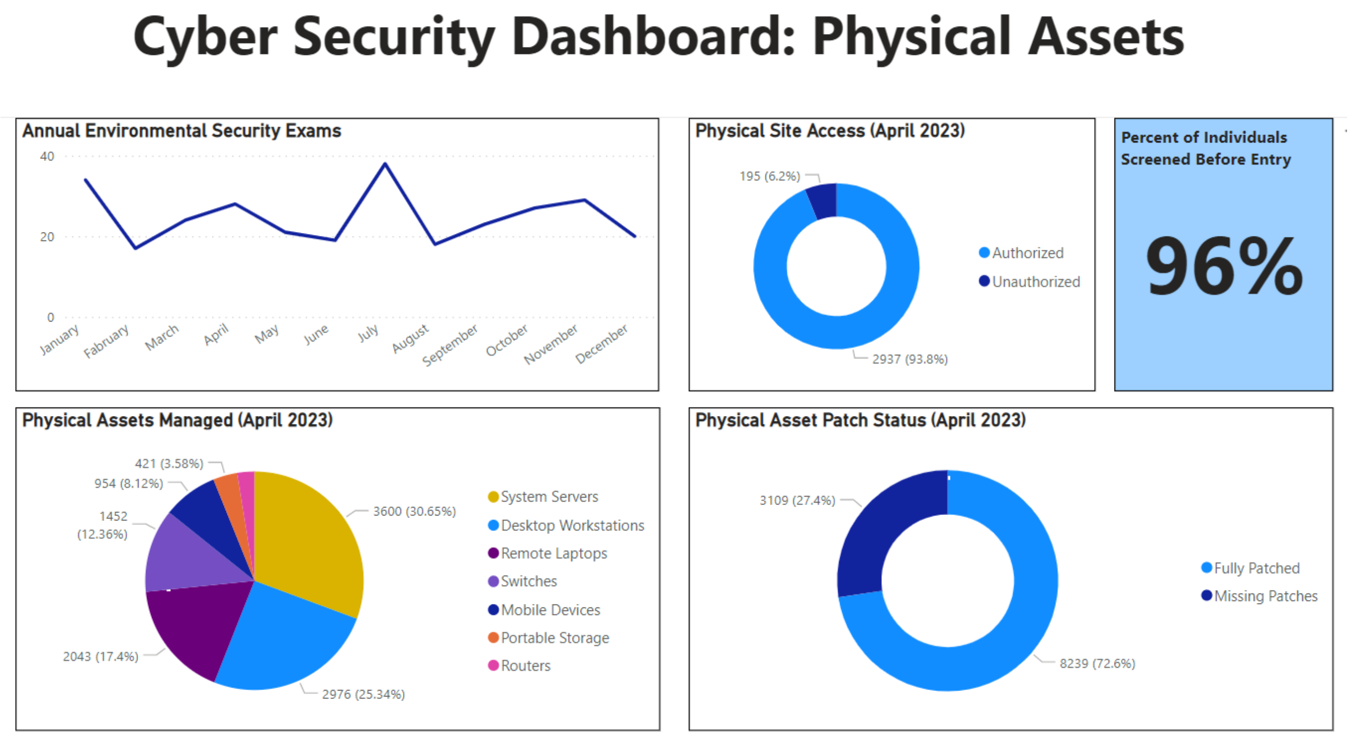
Malware Blocked by Firewall: This metric measures how effective our firewalls are at stopping malware of known signatures from getting into our systems. The data from this metric allows the CISO to determine if malware is bypassing our tools and prioritize fixing that entry point if needed. This metric aligns with ISO 27002 12.2 and 12.6. This metric was chosen to help demonstrate the effectiveness of a primary tool in malware defense of our systems.

Category: Physical Assets

ISO 27002 8.1 Responsibility for Assets

ISO 27002 11.1 Secure Areas

ISO 27002 11.2 Equipment



Metrics:

Annual Environmental Security Exams: This metric provides information on the frequency of security checks on physical sites. These sorts of security checks ensure the physical site is secure from environmental threats and assess the security of physical entry points to the sites. The metric aligns with ISO 27002 11.1/11.2, ensuring the physical areas and equipment are secure from an external perspective.

Physical Assets Managed: This metric displays the various physical assets the organization is responsible for managing. This information helps to visualize the proportions of each asset type managed in a means to aid in resource management. The pie chart visualization was chosen to best differentiate between assets and show the variance between them. This metric aligns with the ISO 27002 8.1 Responsibility for Assets standard.

Physical Site Access: This metric shows the percentage of authorized versus unauthorized access to the physical sites managed. This information aims to help assess the effectiveness of external security of the organization’s physical sites. This metric aligns with ISO 27002 11.1 standard, ensuring the physical site areas are secure.

Physical Asset Patch Status: While we have demonstrated metrics about the physical assets being housed securely, this metric provides information about the security of the software the physical assets are running. With unpatched devices being a strong attack vector of malicious actors, it is important that we measure the upkeep of these patches on the devices. This metric aligns with the ISO 27002 8.1 standard, ensuring that these assets are secured from a software perspective.

Percent of Individuals Screen Before Entry: This metric shows a quick analysis of the percentage of individuals who have, on average, gained access to the organization’s physical sites. This information is used in tandem with the Physical Site Access metric to help analyze if the organization’s screening process is directly related to unauthorized individuals entering the site. This metric aligns with the ISO 27002 11.1 standard.

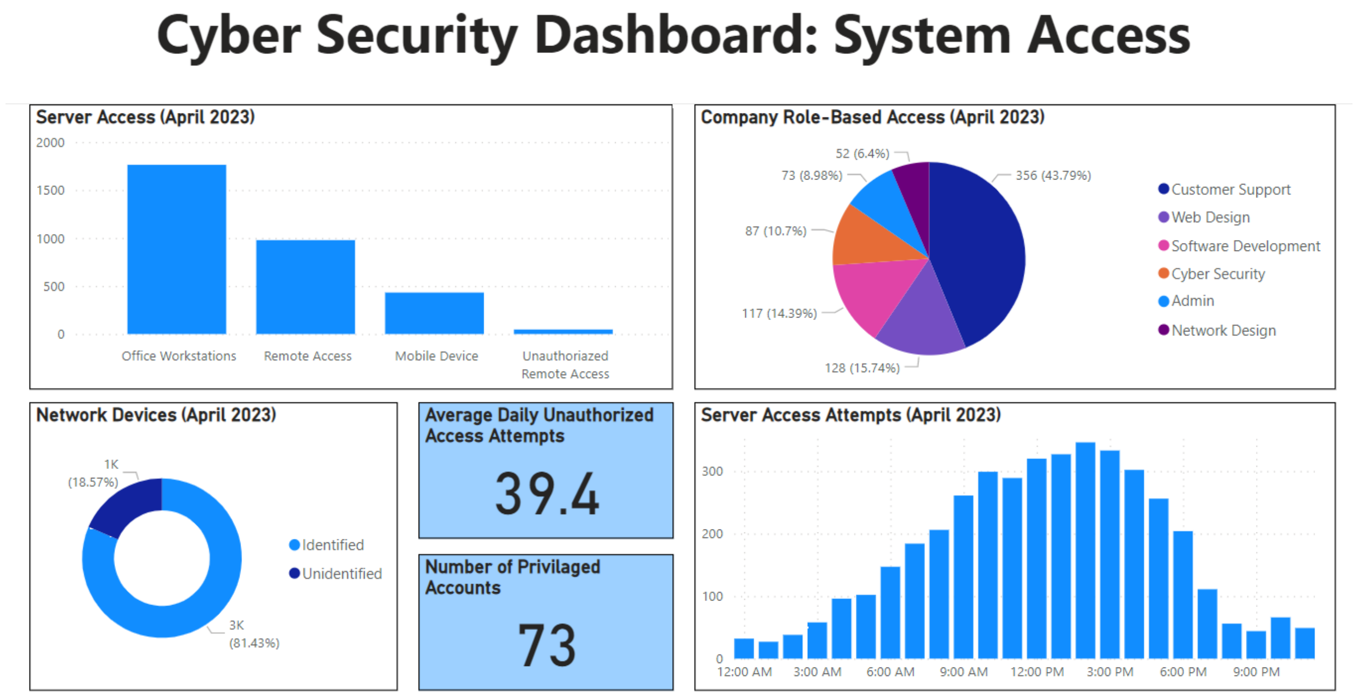
Category: System Access

ISO 27002 9.2 User Access Management

ISO 27002 9.3 User Responsibilities

ISO 27002 9.4 System and Application Access Control

ISO 27002 12.6 Technical Vulnerability Management



Cyber Security Dashboard: System Access

Average Daily Unauthorized Access Attempts

39.4

Number of Privilaged Accounts

73

Metrics:

Server Access: This metric provides information about the variety of devices being used to access server information and the volume each of those device categories is being used to access information. This data can be used to make decisions on where to best focus resources for protecting access control. This metric aligns with the ISO 9.4 metric, helping to make decisions in system access control.

Company Role-Based Access: This metric demonstrates the various roles in the organization being used to access server data. This information helps paint a picture of the responsibilities of different individuals in the organization. The visualization choice was made to show the diversity of the roles and the quantity of each role. This metric aligns with the ISO 27002 9.2 and 9.3 standards, demonstrating the focus on analyzing the responsibilities of the users in the organization.

Network Devices: This metric measures the number of devices on the network that are not properly identified or recognized. It helps identify potential security risks and unauthorized devices that may pose threats or vulnerabilities. By reducing the number of unidentified devices, the organization can maintain better control over its network environment. This metric aligns with ISO 27002 standard, specifically section 12.6 on Technical Vulnerability Management.

Average Daily Unauthorized Access Attempts: This KPI metric shows a quick data point of our systems' daily unauthorized access attempts. This information shows viewers the daily volume of these sorts of threats with the aim of making better decisions about preventing these unauthorized users from gaining access. This metric aligns with the ISO 27002 9.4 standard, ensuring system access control.

Number of Privileged Accounts: This KPI metric shows the number of current accounts in the organization with privileged access control. This specific piece of data is important for security teams to analyze as it highlights the number of accounts that can access the organization's most sensitive data. This metric aligns with the ISO 27002 9.3 and 9.4 standards, focusing on the responsibilities of users and being used to analyze system access control.

Server Access Attempts: This metric provides information on the average traffic the servers handle every hour of the day. This data is helpful for the CISO to make decisions about resource allotment for different parts of the day. The bar graph visualization was chosen to help illustrate the flow of traffic throughout the day. This metric aligns with the ISO 27002 standard.

Category: Security Monitoring

ISO 27001 9.2 Internal Audit

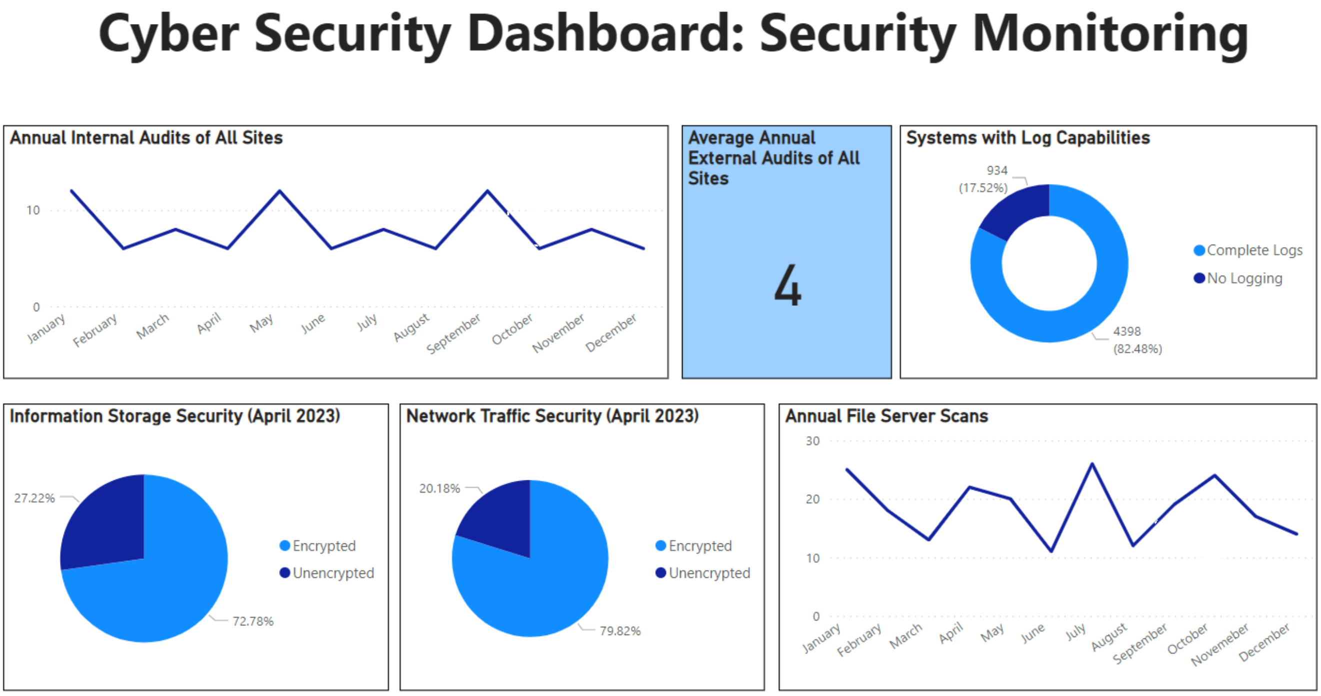
ISO 27002 12.4 Logging and Monitoring

ISO 27002 10.1 Cryptographic Controls

ISO 27002 12.7 Information Systems Audit Considerations

ISO 27002 13.1 Network Security Management

ISO 27002 13.2 Information Transfer



Metrics:

Annual Internal Audits of All Sites: This metric demonstrates the cadence of internal audits the organization performs over a year period. This information is used to ensure the organization is compliant as well as help with analysis of the periodic strength of their security. This metric aligns with the ISO 27001 9.2 standard.

Average External Audits of All Sites: This KPI metric shows the average annual external audits the organization has performed. These pieces of information can be used with the internal audit metric to make decisions about the organization's overall audit plan. This metric aligns with the ISO 27002 12.7 standard.

Systems with Log Capabilities: This metric shows a percentage of systems in the organization with logging capabilities. When monitoring the systems' security, they must be able to log vital information for incident response and analysis. This metric aligns with the ISO 27002 12.4 standard, as it provides data on the logging and monitoring of the systems.

Information Storage/Network Traffic Security: These metrics demonstrate the security of both data being stored in the organization's systems and the data being transferred in its networks. This information helps the CISO make decisions about allocating resources to better protect this data at rest and in transit. These metrics align with the ISO 27002 10.1 standard, providing information about the use of cryptography to protect data in the organization. The latter also aligns with ISO 27002 13.1/2.

Annual File Server Scans: This metric demonstrates how often the organization's file servers are scanned to analyze the proper storage of data. This information can be used by the CISO to make sure systems are being checked promptly and often. This metric aligns with the ISO 27002 12.4 standard.

Technology Architecture and Justification

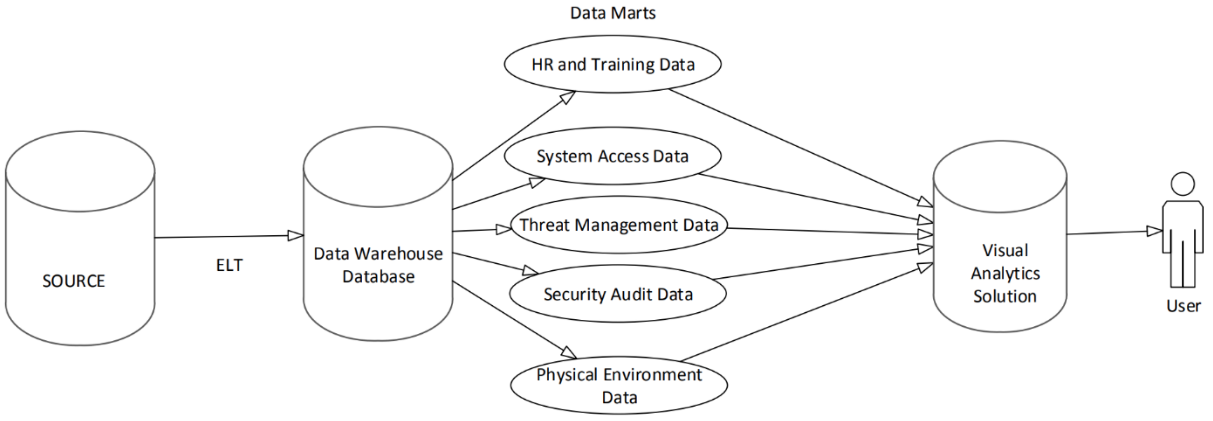


Figure 1. Technology Architecture Diagram

The above figure of the technology architecture diagram shows the technology structure that this system would use, assuming that it makes use of data warehouse technology. To start, the system would receive as input a large amount of data from a source system such as Darktrace. This is shown in the far left of the diagram where there is the server labeled source. This data from the source is then transferred to the data warehouse database using a process called "Extract, Load, Transform" (ELT). ELT was chosen over the "Extract, Transform, Load" (ETL) model of data transfer because ETL would have required an extra server to handle the transformation. This excess hardware would be not only an additional cost to the organization but also a potential security risk, as it would be yet another point at which the data could be compromised. The use of ELT means that the data is then transformed once it reaches the data warehouse database. The data warehouse database is where all the data is stored together in one location. This data is then broken up into subsets on the data warehouse called data marts. These data marts make the access and use of the data by the application much more straightforward by sectioning the data into categories so that it may be located more easily. All of this is then accessed by the application on the web server and used by the user.

This system will support the role of chief information security officer in that it aggregates the vast majority of information they must check in one spot and presents it in an easily digestible manner. In addition, this system supports the certification for ISO 27001 ISMS in that it presents the information on the system to many interested parties with technical expertise. Futhermore, it presents it in such a way that it makes it easier for those individuals to present it to other interested parties who do not have technical expertise, such as the CISO presenting the information to the other executive-level officers of the organization. This ensures that the communication aspects of the ISO 27001 ISMS certification are met. Additionally, this information provided to the CISO and other high-level executives makes it much simpler for them to ensure policies necessary to meet the other requirements of ISO 27001 certification are being fulfilled properly and if any additional policies should be made.