Dashboard Overview

Upon logging in, you'll be greeted by the dashboard, your central hub for monitoring and managing your organization's cybersecurity posture. Here, you'll find a comprehensive overview of the available modules along with key information to help you stay informed and in control.

- Overview
- Risk Score
- CRAM View
- Top Concerns
- Open Cases
- Social Engineering Compromised Users
- Current Cyber Incidents
- Security & Privacy Compliance
- Social Engineering
- Source Destination Map

Overview

1. **Cyber Detection and Response (5 Modules)**: This section provides tools for proactive threat detection and swift response, including Cyber Incident Monitoring, Security Orchestration, Automation and Response, Threat Intelligence, Endpoint Detection and Response, and User and Entity Behavior Analysis.
2. **Cyber Governance (5 Modules)**: Ensure compliance and effective governance with features such as Security Compliance, Privacy Compliance, Governance and Management, Cloud Security Posture Management, and Asset Discovery and Management.
3. **Cyber Risk Management (6 Modules)**: Identify, assess, and manage cyber risks with modules covering Social Engineering, Supply Chain Risk Management, Virtual Penetration Testing, Vulnerability Assessment and Management, Cyber Risk Assessment, and Cyber Risk Management.
4. **Identity and Data Governance (4 Modules)**: Secure identities and data with Privileged Account Review, Data Security Posture Management, Identity and Access Review, and Data Governance tools.
5. **Cyber Resiliency (3 Modules)**: Ensure business continuity and resilience against cyber threats with Business Continuity Management, Disaster Recovery Planning, and Cyber Insurance Analysis.

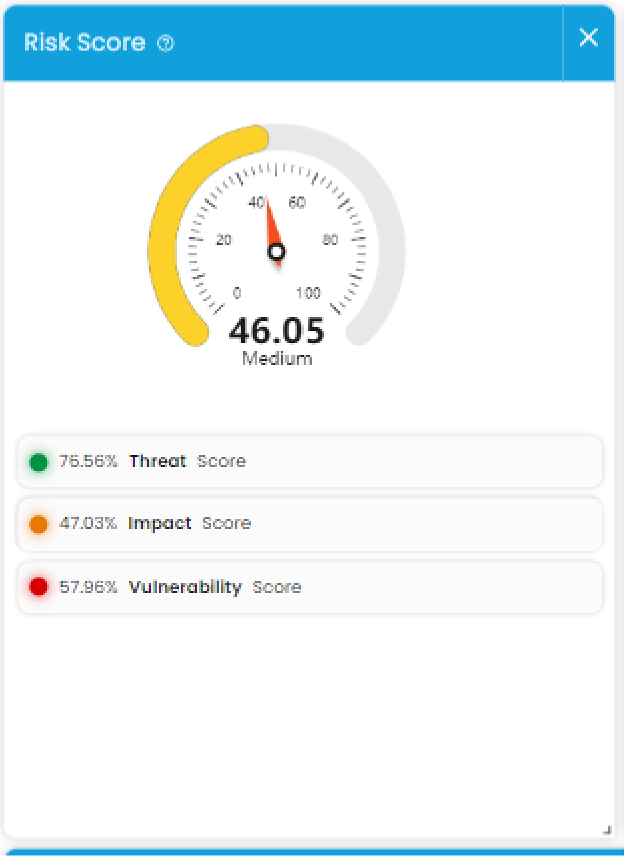
Risk Score

The risk score serves as a comprehensive indicator of your company's overall risk level. This score amalgamates various factors and assessments to provide you with a clear understanding of your organization's cyber security risk posture. It acts as a powerful tool for prioritizing and addressing potential vulnerabilities and threats effectively.

By monitoring the risk score regularly, you can stay proactive in managing cyber security risks and ensuring the resilience of your organization against potential threats. The risk score is dynamically updated based on the latest data and assessments, enabling you to make informed decisions and take timely actions to mitigate risks.

Utilize the risk score as a guiding metric to drive cyber security initiatives, allocate resources efficiently, and continuously improve your organization's security posture. For detailed insights into the factors contributing to the risk score and strategies for risk mitigation, explore the corresponding modules and features within the CISO Workplace Modules.

By leveraging the risk score effectively, you can bolster your organization's cyber resilience and protect its digital assets against evolving threats.



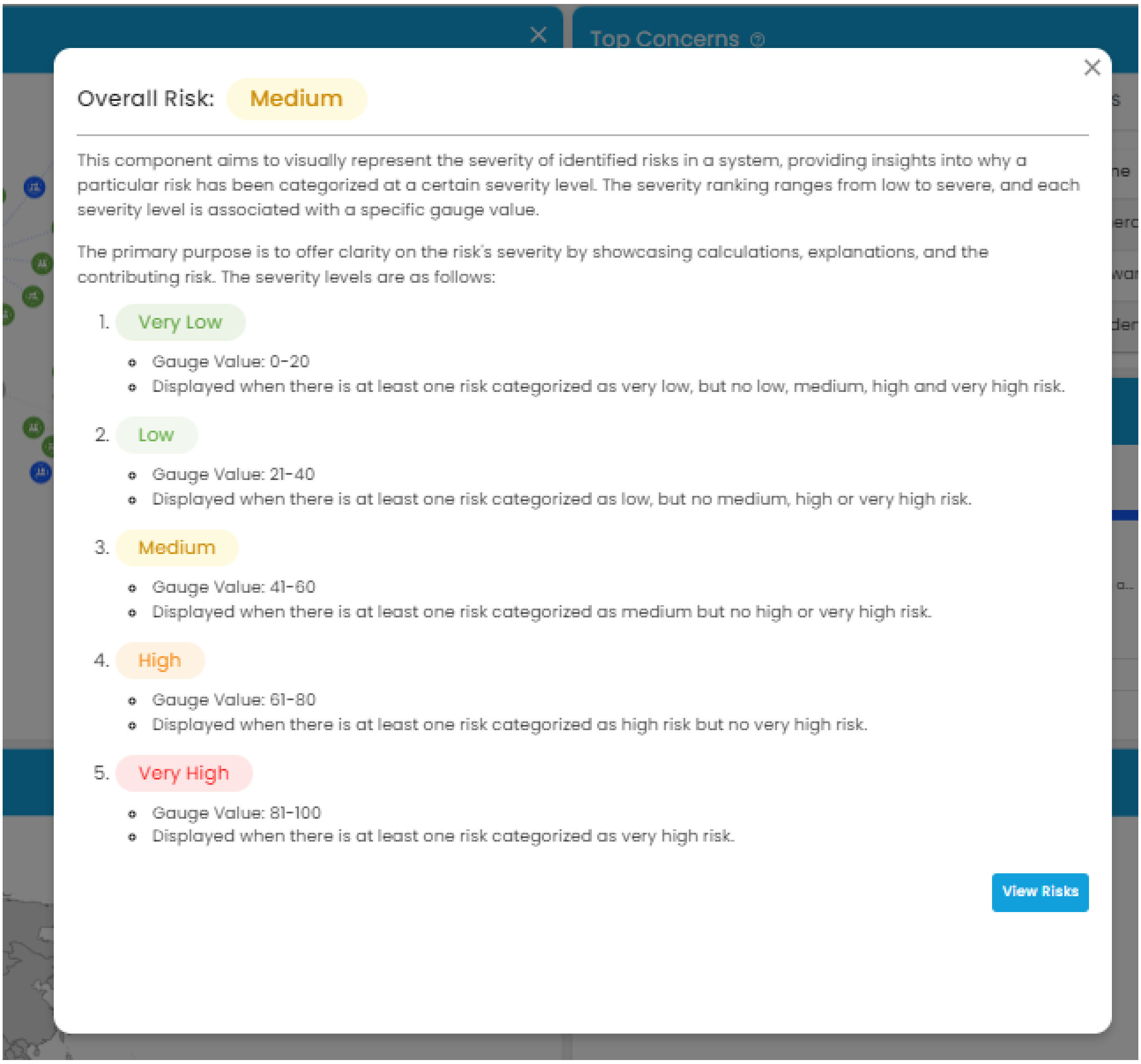
46.05
Medium

● 76.56% **Threat** Score

● 47.03% **Impact** Score

● 57.96% **Vulnerability** Score

Clicking on the risk score will grant you access to a detailed breakdown of the severity levels comprising the overall risk score. This feature offers invaluable insights into the specific areas contributing to your organization's risk posture, enabling you to pinpoint vulnerabilities and prioritize mitigation efforts effectively.



Overall Risk: Medium

This component aims to visually represent the severity of identified risks in a system, providing insights into why a particular risk has been categorized at a certain severity level. The severity ranking ranges from low to severe, and each severity level is associated with a specific gauge value.

The primary purpose is to offer clarity on the risk's severity by showcasing calculations, explanations, and the contributing risk. The severity levels are as follows:

1. Very Low
   - Gauge Value: 0-20
   - Displayed when there is at least one risk categorized as very low, but no low, medium, high and very high risk.
2. Low
   - Gauge Value: 21-40
   - Displayed when there is at least one risk categorized as low, but no medium, high or very high risk.
3. Medium
   - Gauge Value: 41-60
   - Displayed when there is at least one risk categorized as medium but no high or very high risk.
4. High
   - Gauge Value: 61-80
   - Displayed when there is at least one risk categorized as high risk but no very high risk.
5. Very High
   - Gauge Value: 81-100
   - Displayed when there is at least one risk categorized as very high risk.

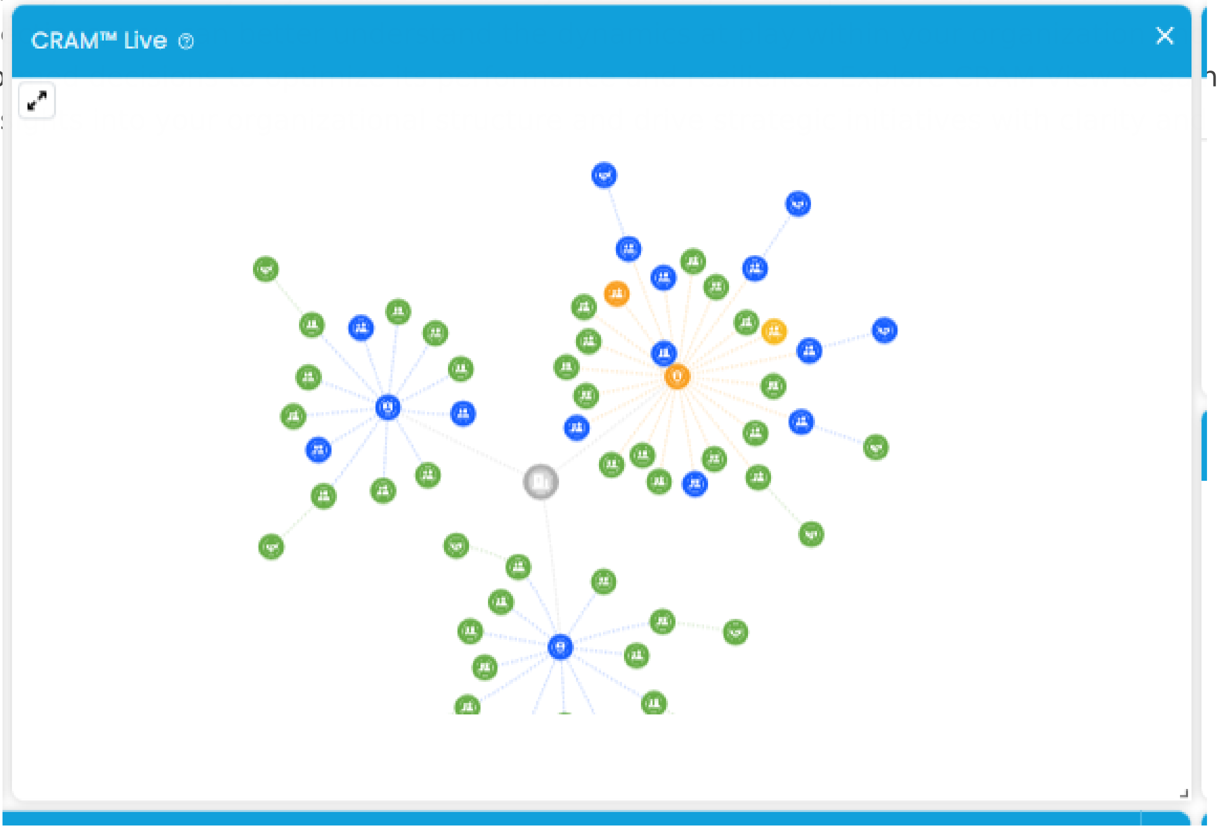
If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

CRAM View

CRAM View provides a dynamic visualization of your organization's structure, offering real-time insights into its critical components and interconnections. Here's a breakdown of what you'll see:

- **Center**: The central element represents your organization, serving as the focal point of the visualization.
- **Three Surrounding Circles**: These circles depict your organization's Critical Business Processes, highlighting the core functions essential for your operations and success.
- **Connected Circles**: Circles connected to the central element represent Critical Business Functions, illustrating the interdependencies and relationships between different aspects of your organization's operations.
- **Other Nodes**: Additional nodes scattered throughout the visualization represent business vectors, capturing various elements and aspects that contribute to your organization's overall structure and functioning.

CRAM View offers a holistic perspective of your organization's architecture, allowing you to grasp
its comple
interconn
make info h
deeper in
precision.

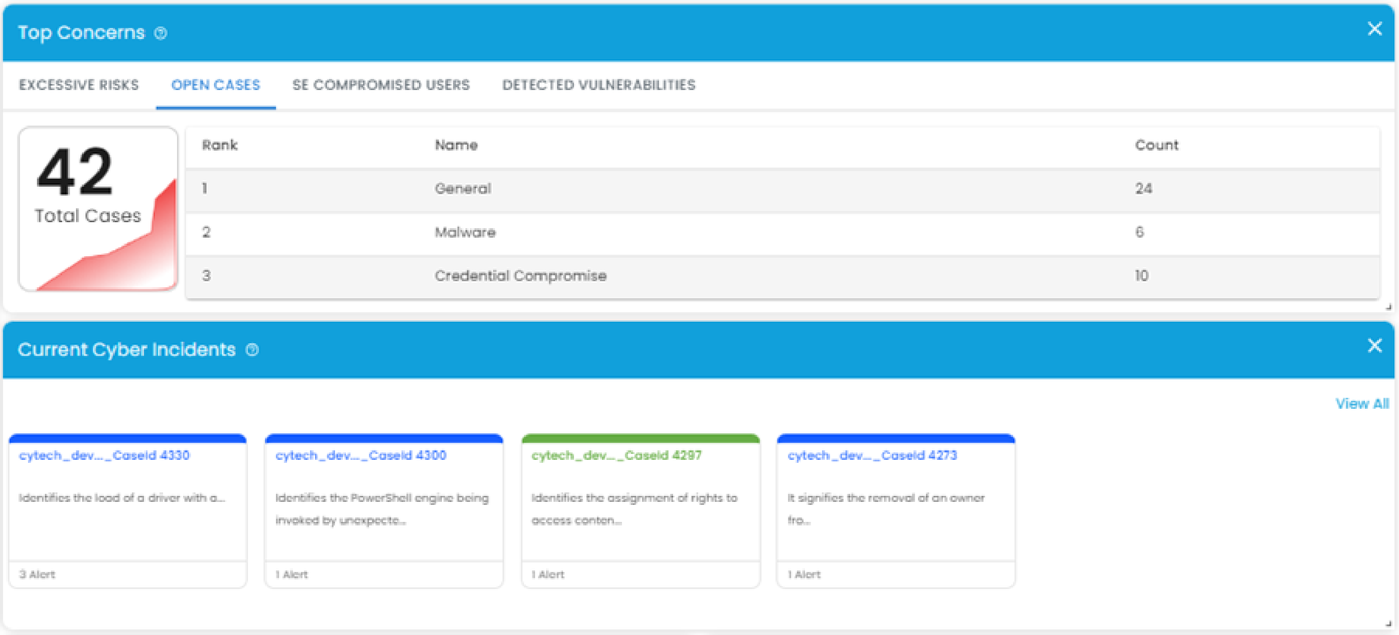


If you need further assistance, kindly contact our support at info@cytechint.com for prompt assistance and guidance.

Top Concerns

This section is dedicated to spotlighting the most critical concerns or issues currently impacting your organization. Here's what you need to know:

- **Focused Attention**: We've curated a list of the top concerns that demand immediate attention, ensuring that you're well-informed about the most pressing issues affecting your organization's cyber security posture.
- **Priority Insights**: By identifying and prioritizing these concerns, we empower you to allocate resources and efforts effectively, addressing vulnerabilities and threats in a timely manner.
- **Risk Awareness**: Understanding the top concerns enables you to enhance risk awareness across your organization, fostering a proactive approach to risk mitigation and resilience-building efforts.
- **Actionable Intelligence**: Each concern highlighted in this section is accompanied by actionable intelligence and recommended steps for mitigation, empowering you to take decisive actions to safeguard your organization's digital assets.



Top Concerns

42
Total Cases

Rank	Name	Count
1	General	24
2	Malware	6
3	Credential Compromise	10

Current Cyber Incidents

cytech_dev..._CaseId 4330
Identifies the load of a driver with a...
3 Alert

cytech_dev..._CaseId 4300
Identifies the PowerShell engine being invoked by unexpecte...
1 Alert

cytech_dev..._CaseId 4297
Identifies the assignment of rights to access conten...
1 Alert

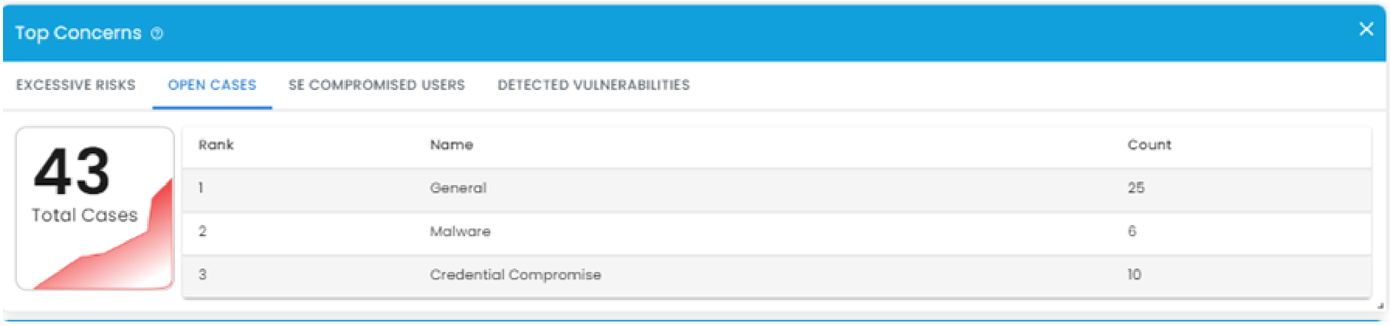
cytech_dev..._CaseId 4273
It signifies the removal of an owner fro...
1 Alert

By staying informed about the top concerns facing your organization, you can proactively manage risks, strengthen your cyber security defenses, and ensure the continuity and resilience of your operations. Explore this section to gain valuable insights and drive strategic initiatives that address your organization's most critical cyber security challenges effectively.

Open Cases

In this section, you'll find a comprehensive overview of open cases within your organization. Here's what you can expect:

- **Organized by Category**: Cases are meticulously sorted by category, offering a clear and structured view of the different types of incidents or issues currently being addressed by your team.
- **Count Indicators**: Each category is accompanied by a count indicator, providing a quick snapshot of the number of open cases associated with that particular category. This allows you to gauge the magnitude of issues within each category at a glance.
- **Efficient Prioritization**: With cases organized by category and accompanied by count indicators, you can prioritize your team's efforts more efficiently, focusing on resolving high-impact issues first while ensuring that all cases receive appropriate attention.
- **Streamlined Management**: This organized approach to case management streamlines your workflow, making it easier to track, monitor, and address incidents in a timely manner, ultimately enhancing your organization's ability to respond effectively to cybersecurity threats and challenges.



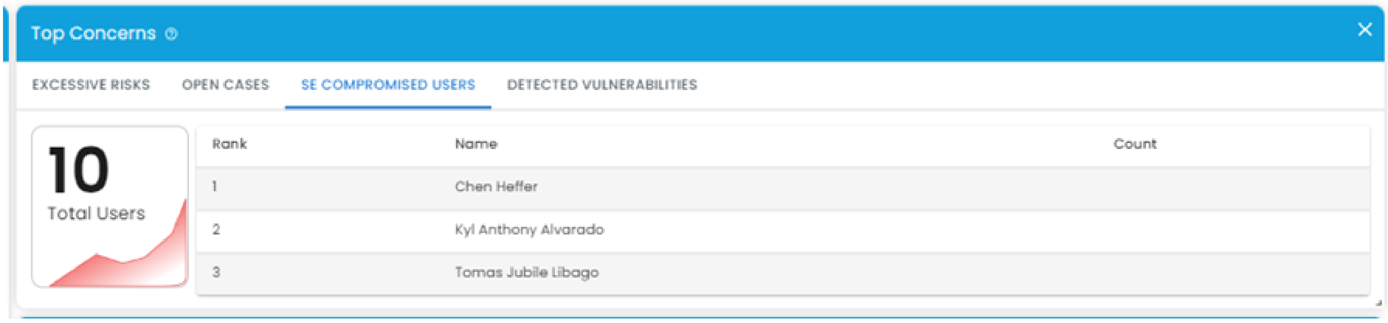
Rank	Name	Count
1	General	25
2	Malware	6
3	Credential Compromise	10

By leveraging the insights provided in the Open Cases section, you can optimize your team's response efforts, mitigate risks more effectively, and maintain a proactive stance in safeguarding your organization's assets and data. Explore this section to stay informed about ongoing cases and take decisive action to address cyber security incidents promptly.

Social Engineering Compromised Users

In this section, you'll find vital information regarding users who have recently fallen victim to phishing simulations, offering valuable insights into potential vulnerabilities within your organization's cyber security defenses. Here's what you need to know:

- **Top Compromised Users**: The section presents a concise list of the top three users who have recently failed phishing simulations, highlighting individuals who may be particularly susceptible to social engineering attacks.
- **Recent Activity**: By focusing on recent incidents, you can stay informed about the latest trends and patterns in social engineering attempts, allowing you to take proactive measures to mitigate risks and enhance user awareness and training.
- **Targeted Intervention**: Identifying compromised users enables you to provide targeted support and additional training to enhance their resilience against social engineering tactics, reducing the likelihood of future breaches and strengthening your organization's overall security posture.
- **Risk Mitigation**: By addressing vulnerabilities at the individual user level, you can mitigate the risk of successful social engineering attacks, safeguarding sensitive data and protecting your organization from potential security breaches.



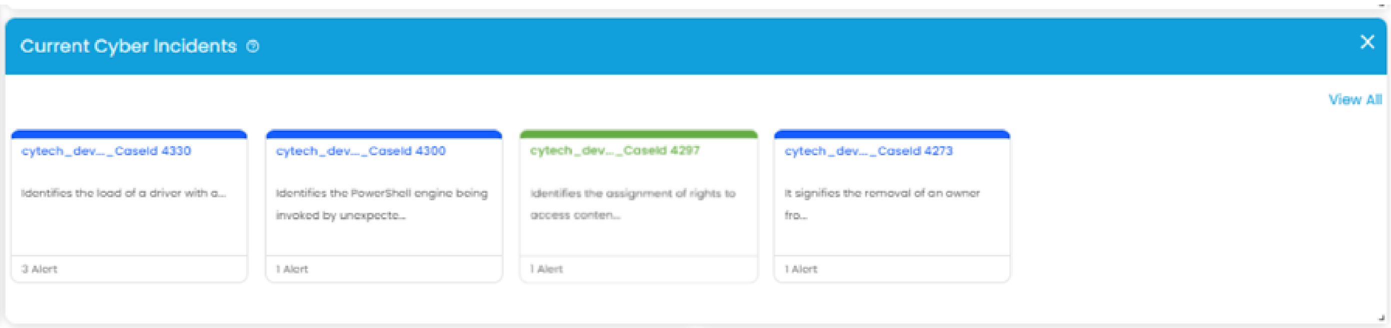
Rank	Name	Count
1	Chen Heffer	
2	Kyl Anthony Alvarado	
3	Tomas Jubile Libago	

This section serves as a valuable tool for risk assessment and mitigation, empowering you to address weaknesses in user awareness and behavior and fortify your organization's defenses against social engineering threats. Explore this section to stay vigilant and proactive in safeguarding your organization's assets and data against evolving cybersecurity risks.

Current Cyber Incidents

Stay informed about the latest cyber incidents detected by our CIMS Module/Platform with this essential section. Here's what you'll find:

- **Real-Time Updates**: Get up-to-the-minute information on the most recent cyber incidents identified by our CIMS Module/Platform, ensuring you stay ahead of emerging threats and vulnerabilities.
- **Detailed Insights**: Each incident is accompanied by detailed insights, including the nature of the incident, affected systems or assets, severity level, and recommended actions for mitigation.
- **Timely Response**: With real-time visibility into current cyber incidents, you can initiate prompt response actions, such as containment, investigation, and remediation, to minimize the impact on your organization's operations and data security.
- **Continuous Monitoring**: By monitoring current cyber incidents, you can identify patterns and trends, enabling proactive measures to enhance your organization's cyber resilience and prevent future incidents.



cytech_dev..._CaseId 4330

Identifies the load of a driver with a...

3 Alert

cytech_dev..._CaseId 4300

Identifies the PowerShell engine being invoked by unexpecte...

1 Alert

cytech_dev..._CaseId 4297

Identifies the assignment of rights to access conten...

1 Alert

cytech_dev..._CaseId 4273

It signifies the removal of an owner fro...

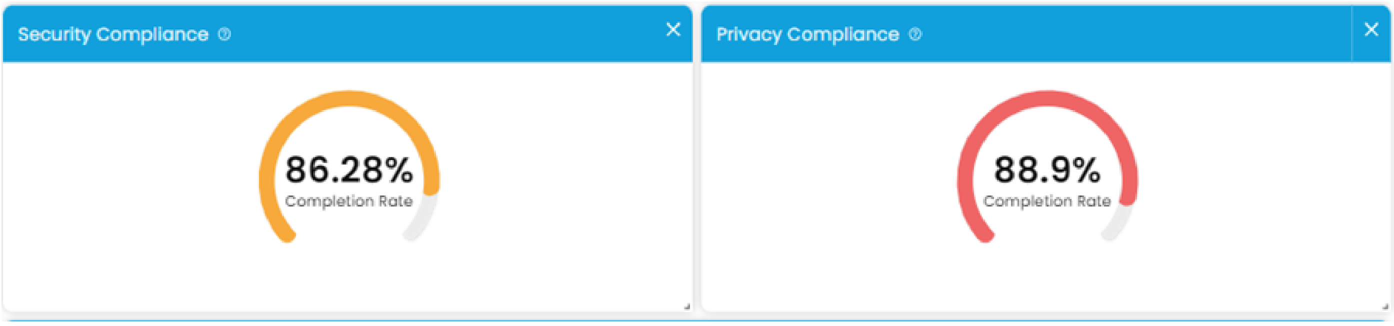
1 Alert

This section serves as a central hub for monitoring and managing cyber incidents, empowering you to take swift and decisive action to protect your organization's assets and maintain operational continuity in the face of evolving cyber security threats. Explore this section to stay informed, proactive, and resilient in the ever-changing landscape of cyber threats.

Security & Privacy Compliance

This section provides a comprehensive overview of your organization's current status regarding security and privacy compliance. Here's what you can expect:

- **Percentage Completion**: Gain insight into the current percentage completion of compliance requirements, allowing you to track progress and ensure alignment with regulatory standards and best practices.
- **Detailed Information**: Clicking on each module redirects you to the respective compliance module, where you can access detailed information, documentation, and resources related to security and privacy compliance.
- **Streamlined Navigation**: Seamlessly navigate between modules to access the specific compliance areas relevant to your organization, facilitating efficient management and monitoring of compliance efforts.
- **Actionable Insights**: Leverage the information provided to identify gaps in compliance, prioritize remediation efforts, and maintain a robust security and privacy posture to safeguard sensitive data and meet regulatory obligations.

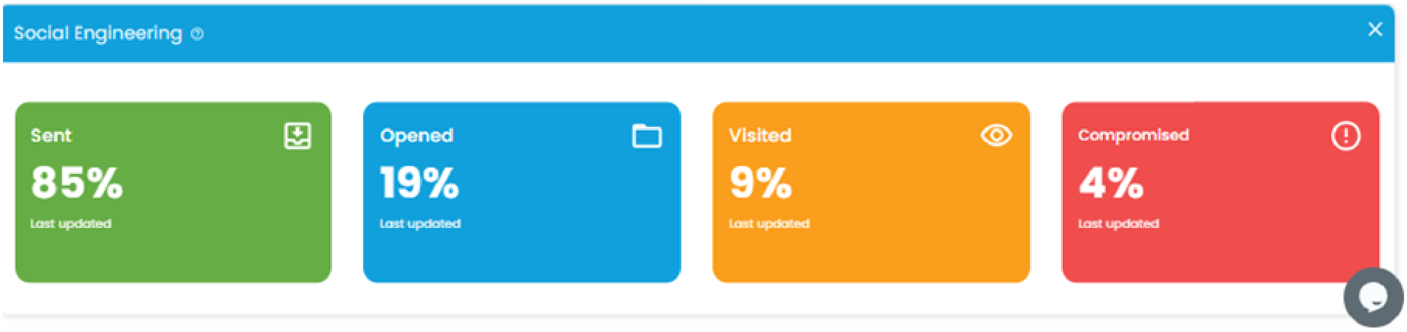


By utilizing this section, you can stay informed, proactive, and well-prepared to address security and privacy compliance requirements effectively. Explore the modules to access valuable resources and guidance that will support your organization in achieving and maintaining compliance excellence.

Social Engineering

This section offers a comprehensive overview of your organization's resilience against social engineering attacks, particularly simulated phishing campaigns. Here's what you can expect:

- **User Engagement Metrics**: Gain insights into user behavior during simulated phishing campaigns, including the percentage of users who have opened, visited, and compromised by interacting with simulated phishing emails.
- **Quantitative Analysis**: Track the effectiveness of your organization's security awareness training and phishing simulation programs by analyzing user engagement metrics, allowing you to measure progress over time and identify areas for improvement.
- **Risk Assessment**: Assess the susceptibility of your workforce to social engineering attacks and prioritize training efforts based on the percentage of compromised users, ultimately strengthening your organization's defenses against real-world threats.
- **Educational Opportunities**: Use the data provided to tailor targeted training initiatives, educate users about the dangers of phishing, and promote a culture of cyber security awareness and vigilance across your organization.

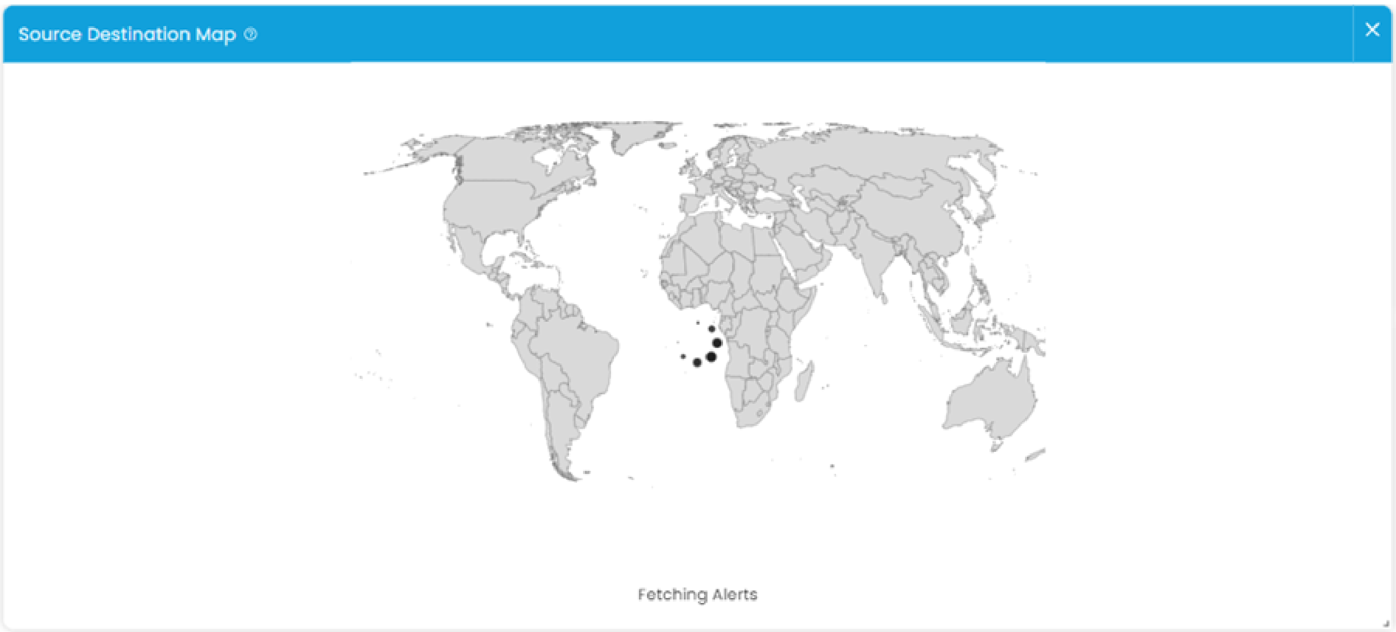


By leveraging this section, you can proactively address vulnerabilities related to social engineering, empower users to recognize and report phishing attempts, and bolster your organization's overall resilience to cyber threats. Explore the insights provided to refine your security awareness training programs and enhance your organization's security posture.

Source Destination Map

This section provides a visual representation of the geographical locations from which attackers commonly originate, offering valuable insights into potential cybersecurity threats faced by your organization. Here's what you can expect:

- **Visual Insights**: Explore an interactive map that visually illustrates the countries from which attackers commonly originate, providing a clear understanding of the geographic distribution of cyber threats targeting your organization.
- **Geospatial Analysis**: Gain actionable intelligence by analyzing the source-destination relationships depicted on the map, enabling you to identify patterns, trends, and emerging threat actors associated with specific geographic regions.
- **Strategic Decision-Making**: Use the insights gleaned from the source-destination map to inform strategic decision-making processes, such as threat prioritization, resource allocation, and the implementation of targeted cyber security measures.
- **Enhanced Situational Awareness**: Enhance your organization's situational awareness by staying informed about the global landscape of cyber threats and understanding the potential risk posed by attackers from various geographical locations.



By leveraging this section, you can enhance your organization's cyber defense strategy, proactively mitigate emerging threats, and strengthen your resilience against cyber attacks originating from different parts of the world. Explore the source-destination map to gain valuable insights and make informed decisions to protect your organization's assets and data.