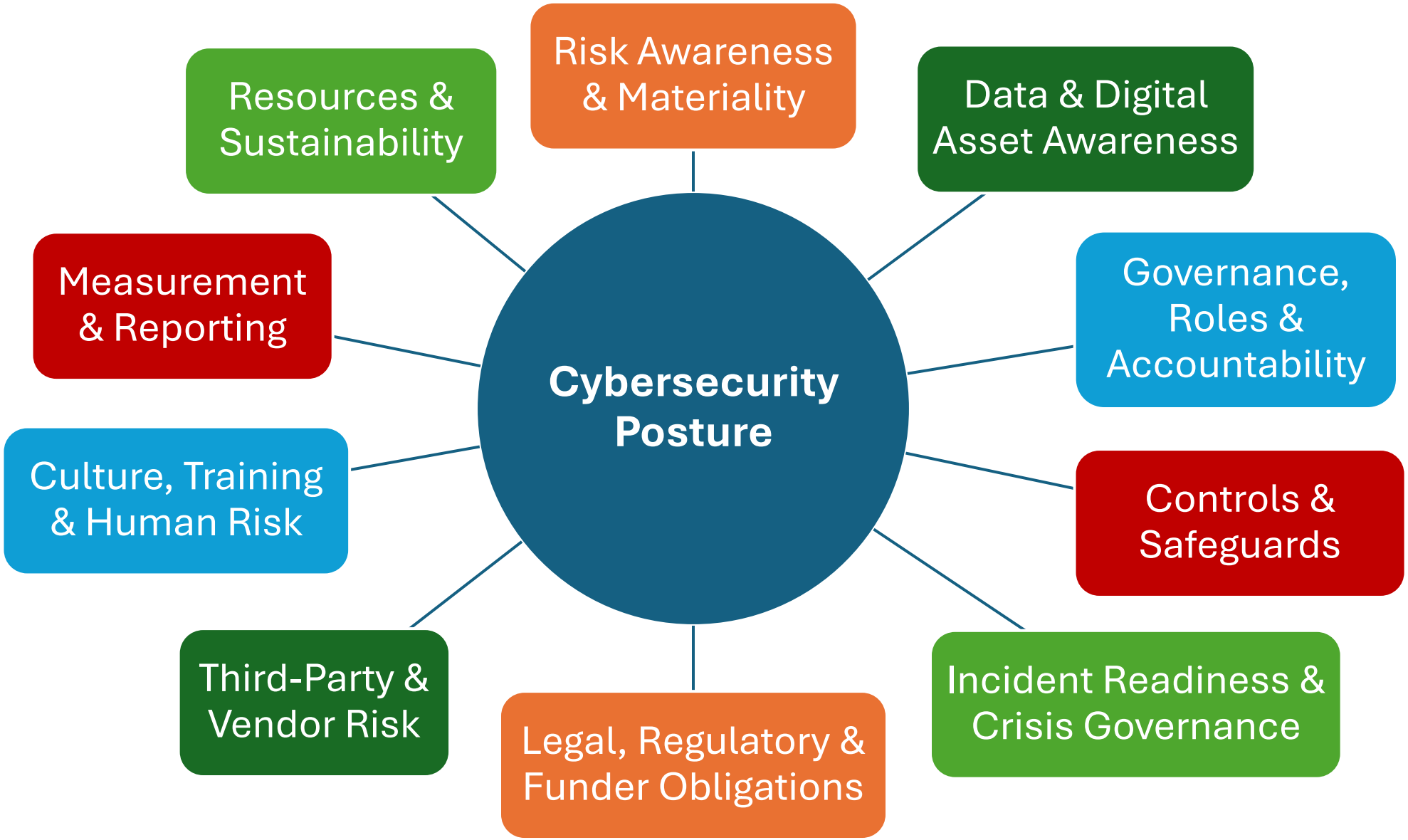
EverSecure Cybersecurity System for the Arts Sector


Cybersecurity Posture
Risk Awareness & Materiality
Data & Digital Asset Awareness
Governance, Roles & Accountability
Controls & Safeguards
Incident Readiness & Crisis Governance
Legal, Regulatory & Funder Obligations
Third-Party & Vendor Risk
Culture, Training & Human Risk
Measurement & Reporting
Resources & Sustainability

Risk Awareness & Materiality

Which cyber risk would cause the most damage to trust with your donors or beneficiaries?

Data & Digital Asset Awareness

Could your organization clearly explain what sensitive data it holds, where it is stored, and who has access to it?

Governance, Roles & Accountability

If the ED/CEO were unavailable during a cyber incident, who would be accountable for the response?

Controls & Safeguards

Is the board confident that management has implemented baseline protections proportionate to the organization's risk profile?

Incident Readiness & Crisis Governance

It's Friday evening and donor data may have been exposed, does your board know what happens next?

Legal, Regulatory & Funder Obligations

Would a data breach today expose the organization to regulatory penalties or funding clawbacks that the board has not yet discussed?

Third-Party & Vendor Risk

If your most critical vendor were breached tomorrow, does the organization have a plan to continue operating?

Culture, Training & Human Risk

Is cybersecurity awareness treated as a shared responsibility across the organization, or does it rest with one person or team?

Measurement & Reporting

Could the board describe the organization's current cybersecurity posture based on the reporting it receives?

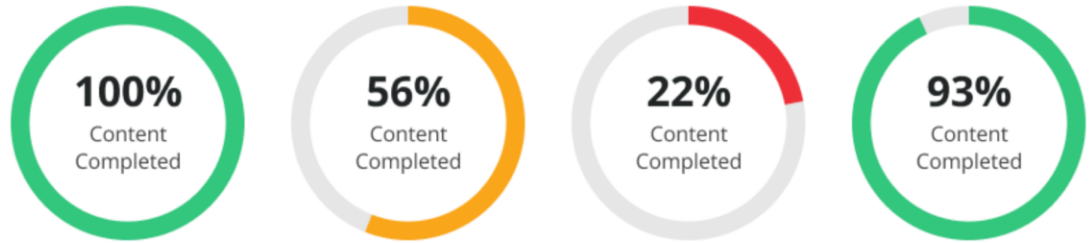
Resources & Sustainability

Is your organization devoting adequate resources to cybersecurity relative to the risks it faces, and what would it take to make that investment sustainable?

EverSecure Dashboard

TOTAL NO. OF VULNERABILITIES

TRAINING CAMPAIGN



SECURITY CONTROLS AUDIT

CIS CSAT Score

INDUSTRIAL AVERAGE: 32

RISK MITIGATION STATUS

THREAT DESCRIPTION	RISK LEVEL	MITIGATION RESPONSE
Management interface exposed https://142.93.154.170:443/wp=login.php	Medium	The remote host is running a management interface exposed to the internet with no access restriction
The site uses some vulnerable javascript libraries.	Medium	Upgrade the library to higher (possibly the latest) version

PHISHING CAMPAIGN

Most recent

DATE	RECIPIENTS	DELIVERED	OPENED	CLICKED	QR CODE SCANNED	REPLIED	ATTACHMENT OPENED
DEC 19, 2023	32	31	15	4	0	0	0
SEP 14, 2023	30	29	15	0	0	0	0
MAY 15, 2023	24	23	10	0	0	0	0
JAN 17, 2023	23	22	15	6	0	0	0

CYBER SECURITY POLICIES

Essential cyber security measures, covering software installation to email protocols.

View details >

INCIDENT RESPONSE PLAN

*LAST UPDATED: NOV 2023

DATA ASSET INVENTORY

*LAST UPDATED: NOV 2023

RISK REGISTER

*LAST UPDATED: NOV 2023

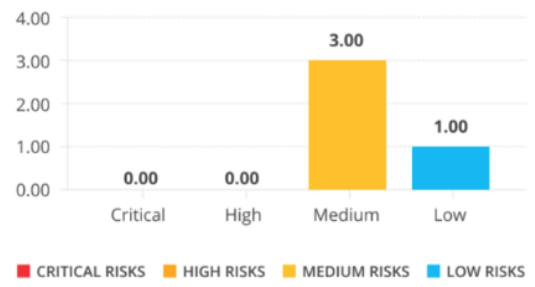
UPCOMING ACTIVITIES

*LAST UPDATED: NOV 2023

EverSecure Dashboard

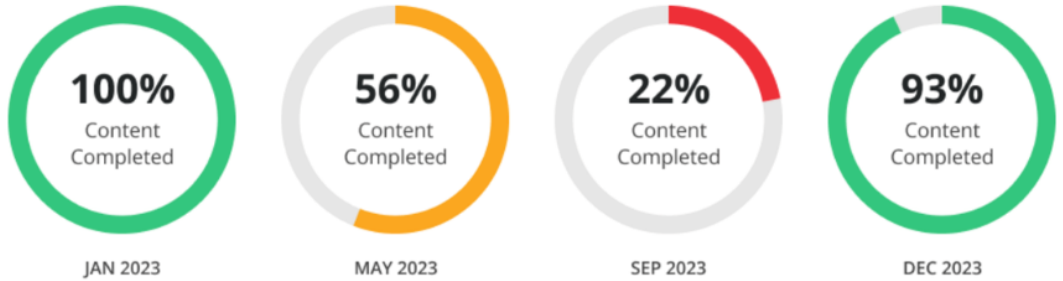
TOTAL NO. OF VULNERABILITIES

1



TRAINING CAMPAIGN

2



SECURITY CONTROLS AUDIT

3

INDUSTRIAL AVERAGE: 32

RISK MITIGATION STATUS

4

THREAT DESCRIPTION	RISK LEVEL	MITIGATION RESPONSE
Management interface exposed https://142.93.154.170:443/wp=login.php	Medium	The remote host is running a management interface exposed to the internet with no access restriction
The site uses some vulnerable javascript libraries.	Medium	Upgrade the library to higher (possibly the latest) version

PHISHING CAMPAIGN

Most recent

2

DATE	RECIPIENTS	DELIVERED	OPENED	CLICKED	QR CODE SCANNED	REPLIED	ATTACHMENT OPENED
DEC 19, 2023	32	31	15	4	0	0	0
SEP 14, 2023	30	29	15	0	0	0	0
MAY 15, 2023	24	23	10	0	0	0	0
JAN 17, 2023	23	22	15	6	0	0	0

CYBER SECURITY POLICIES

5

Essential cyber security measures, covering software installation to email protocols.

View details >

INCIDENT RESPONSE PLAN

6

*LAST UPDATED: NOV 2023

DATA ASSET INVENTORY

7

*LAST UPDATED: NOV 2023

RISK REGISTER

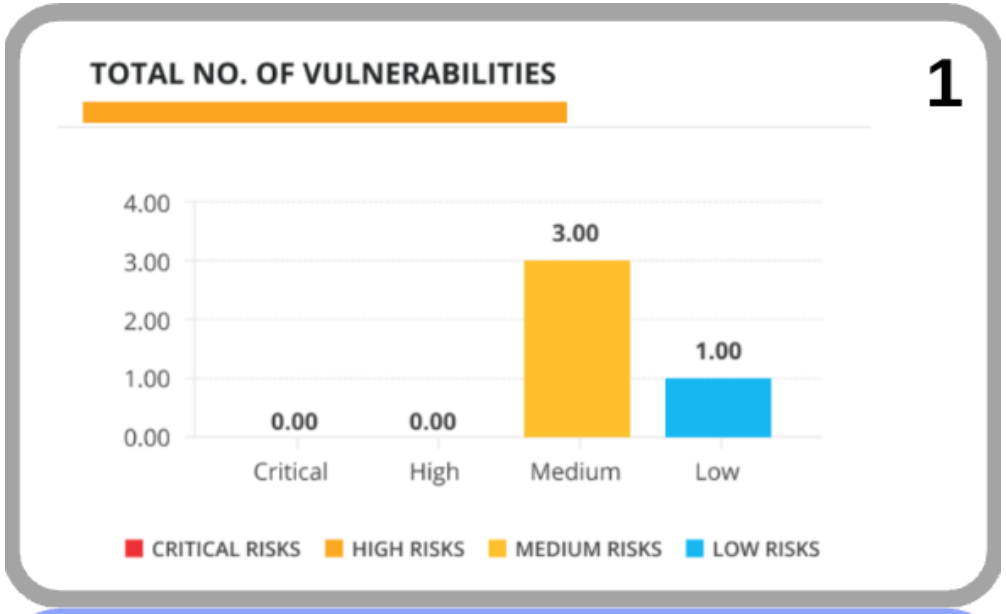
8

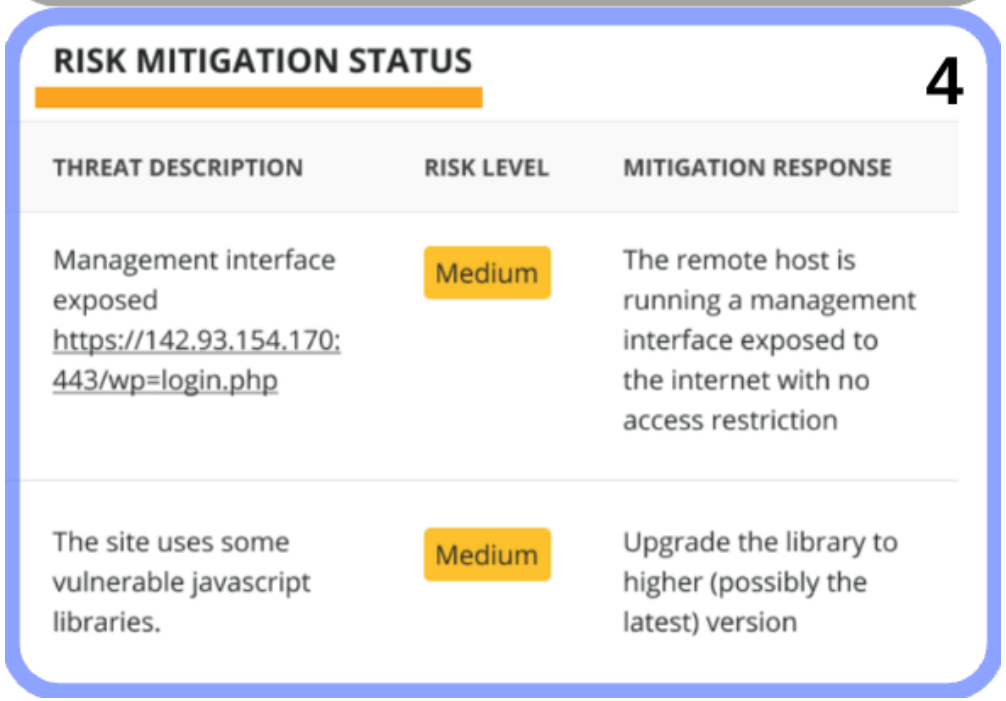
*LAST UPDATED: NOV 2023

UPCOMING ACTIVITIES

9

*LAST UPDATED: NOV 2023



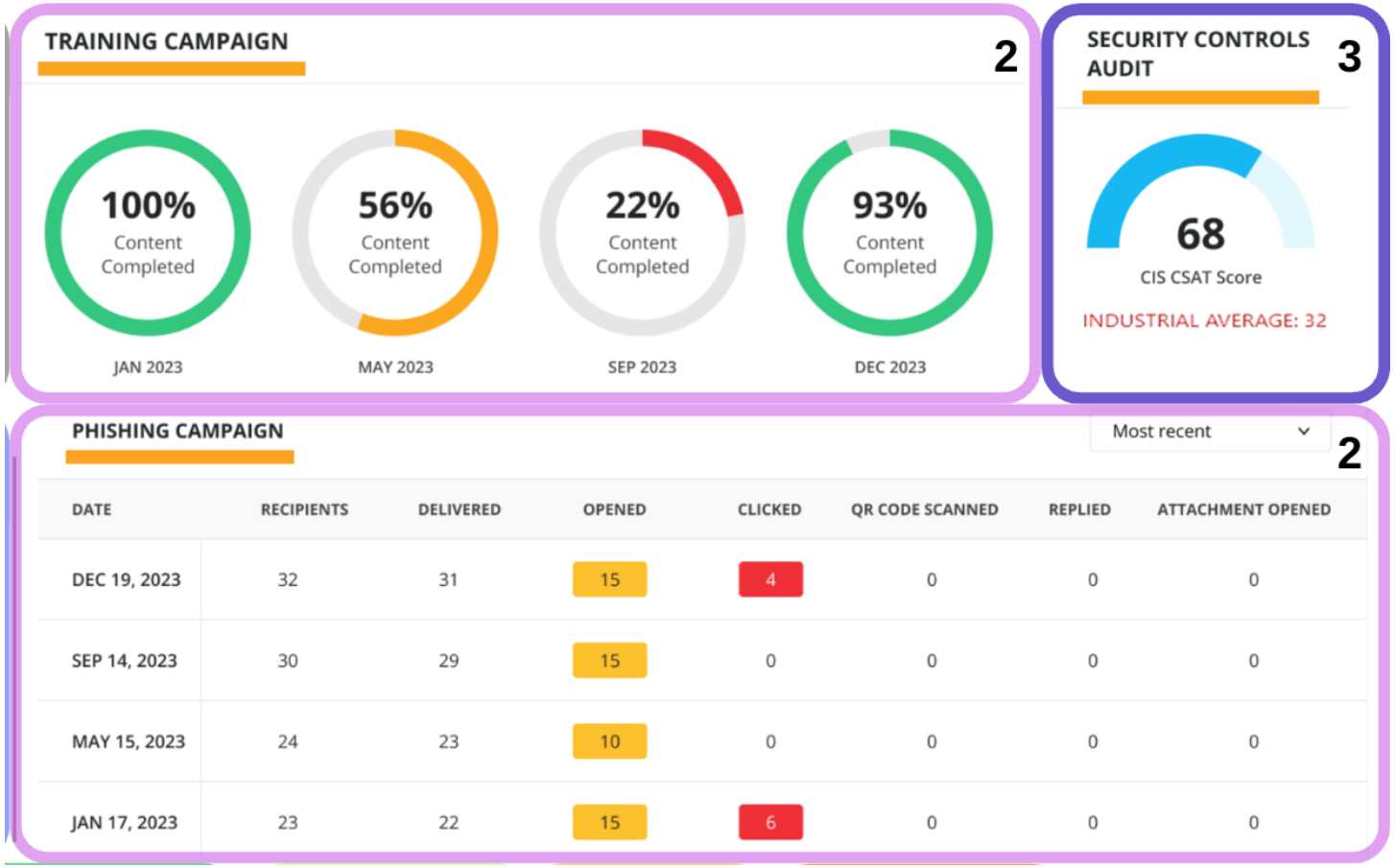


1) Total Number of Vulnerabilities

Shows **current vulnerabilities** by severity, linking scan results to clear risk levels so leaders can see where exposure is concentrated

4) Risk Mitigation Status

Summarizes the **risk findings, risk rating**, and the resolution so you can track how risks are being addressed



3) Security Controls Audit

Displays your **real-time CIS CSAT security controls** score against the industry average, giving a high-level indicator of overall control maturity

2) Training Campaign and Phishing Campaign

Shows **completion rates** for security awareness training and phishing simulation results (opens, clicks, and reporting), giving a single view of staff engagement and human-factor risk

5) Cybersecurity Policies

IT and security policies covering secure software use, email protocols, device management, and data handling to ensure compliance and reduce risk

6) Incident Response Plan

Outlines how the organization manage security incidents, including organizational structure, roles, responsibilities, preparedness, detection, containment, eradication, recovery, and post-incident evaluation

7) Data Asset Inventory

Catalogues all key systems and data assets, including where sensitive information is processed and stored

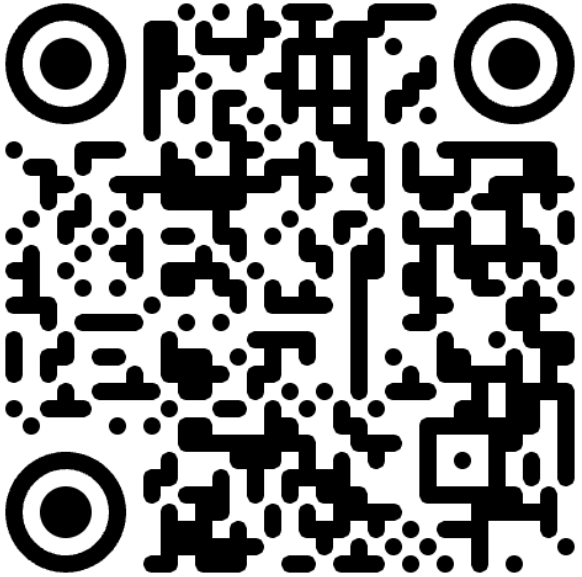
8) Risk Register

Assessment of the data utilized by the organization, evaluation of its value and security measures, and analysis of potential risks

9) Upcoming Activities

Highlights scheduled security initiatives and reviews for leadership to anticipate major milestones and resource needs

Complete Your Cybersecurity Assessment



technologyhelps.org/eversecure

Sign Up for the EverSecure System!

rozsafoundation.com/cybersecurity

Comprehensive Cybersecurity System

Security Analysis and Data Controls

Data Asset and Systems Inventory

Listing and monitoring of all data assets processed, stored, or transferred across the network, implementation of access controls, and regular audits.

Risk Analysis and Assessment

Assessment of the data utilized by the organization, evaluation of its value and security measures, and analysis of potential risks.

Threat Identification, Vulnerability Management, and Reporting

Thorough analysis of external endpoints and internal devices to determine potential risks and required protection levels. Includes device discovery, vulnerability scans, and plans to address identified vulnerabilities.

Controls Audit

Regular reviews of cybersecurity controls and practices, and provision of solutions to enhance the security and confidentiality of digital assets.

Dark Web Monitoring

Continuous monitoring of the dark web to identify whether any employee credentials have been exposed or stolen on the dark web. Detect potential compromises early, reduce the risk of unauthorized access, and take immediate steps such as password resets or additional security measures to protect the organization’s systems and data.

Strategic Planning

IT Policies Evaluation and Development

Evaluation of existing IT policies and controls, addressing compliance gaps, development of necessary new policies and periodic re-evaluation post significant infrastructure changes.

Incident Response Plan and Incident Management

A comprehensive partnership in strategy development and response for managing security incidents, including organizational structure, roles, responsibilities, preparedness, detection, containment, eradication, recovery, and post-incident evaluation.

Tabletop Exercise Implementation

Creation and facilitation of tailored exercise scenarios to simulate potential incidents, involving key personnel and stakeholders to practice the incident response plan.

Backup and Disaster Recovery Planning

Design and implementation of robust backup and disaster recovery plans, including regular drills to ensure business continuity in the event of data loss or disaster.

EverSecure Dashboard

Deployment of the EverSecure Dashboard to centralize security governance metrics, including training outcomes, vulnerability management, risk levels, mitigation efforts, and audit scores.

User Awareness

Cybersecurity Training Program

An advanced online cybersecurity training program aimed at enhancing employee awareness and protection against social engineering and phishing threats. Includes customized training modules and phishing campaigns.

Phish Alert Button Implementation

Integration of a PhishAlert Button within email systems, allowing users to report suspicious emails easily. This triggers an automated IT security ticket for immediate action and helps in blocking future communications from the sender.

Awareness Education and Phishing

Conduct quarterly end-user security training and phishing simulations, including configuration, monitoring, results analysis and gathering user feedback.