



Cygienic vCISO Services

The First 20 days of a Hyper-Performing vCISO

Preface

Cygienic vCISO service is intended for CISOs, Cyber consultants, technology managers, cyber enthusiasts, learners, and other senior security professionals responsible for overseeing an organization's cybersecurity posture. The first 20 days of a Cygienic vCISO job will vary by company, and our tasks may not be feasible within the time frame. We have set an aggressive target, and the assumption is information, people and time is available.



Table of Contents

1. The First 20 days of a Hyper-Performing CISO

- 1 to 5 days :Understand the landscape
- 6 to 10 days :Gaining Cybersecurity Insights
- 11 to 13 days :Developing the Strategy & Thresholds
- 14 to 17 days :Remediation Planning
- 18 to 20 days :Implementation & Continuous Monitoring

2. Getting Started with Cygienic.com vCISO

- Overview
- Accessing the Platform
- Account Setup
- User Interface Overview

The First 20 days of a Hyper-performing vCISO

The First Month

The first 20 days in this position are crucial for setting the tone and establishing a strong foundation for your tenure. This period is about understanding your organization's security landscape, building relationships, and creating a strategic roadmap for cybersecurity.

***Accelerate your progress, by demonstrating to stakeholders
your efficiency and effectiveness in just 20 days.***

Days 1-5: Understand the Landscape

Meet Key Stakeholders (days 1-2)

Executive Team: Schedule meetings with the CEO, CFO, CTO, and other executives to understand their expectations, concerns, and vision for cybersecurity.

IT and Security Teams: Get to know your direct reports and key team members. Understand their roles, responsibilities, and current projects.

Business Unit Leaders: Meet with leaders of various business units to understand their operations, key assets, and how cybersecurity impacts their functions.

Gather Existing Security Data (days 3-4)

Existing Policies and Procedures: Examine current security policies, standards, and procedures. Identify gaps and areas for improvement.

Security Tools and Technologies: Take inventory of the security tools and technologies in use. Understand their effectiveness and any integration challenges.

Critical Assets: Identify the organization's most critical assets, and vendors, including data, systems, and intellectual property.

Incident Response Plans: Review incident response plans and recent incident reports. Assess the organization's readiness to handle security breaches.

Understand the Business (day 5)

Organizational Structure: Familiarize yourself with the company's structure, culture, and key business processes.

Regulatory Requirements: Understand the regulatory landscape and compliance requirements relevant to your industry.

Days 6-10: Gaining Cybersecurity Insights

Collate Company Assets & Critical Suppliers (day 6)

To efficiently manage your assets and vendors, centralize your company names, domains, and vendors within the Cygienic platform. This can be done through the 'Admin Panel' or by requesting pre-population from Cygienic support.

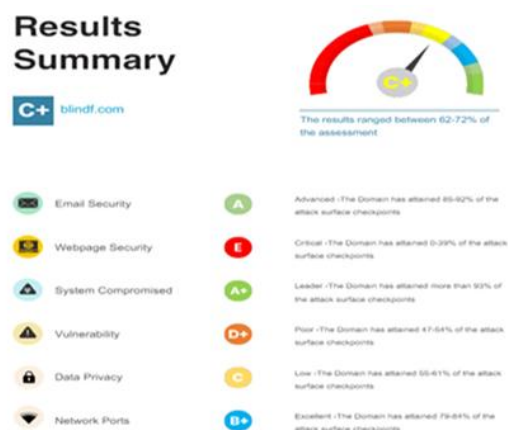
The screenshot displays the Cygienic Admin Panel interface. On the left is a navigation menu with categories like 'Attack Surface', 'System Compromised', 'Vulnerability', 'Data Privacy', and 'Network Ports'. The main content area is titled 'Create Company and Assign Domains' and is divided into three steps: 'Step 1: Create Company', 'Step 2: Assign domains to company', and 'Step 3: Assign company to user'. Each step contains form fields for inputting company details, domains, and users, with 'GO BACK' and 'NEXT' buttons at the bottom of each section.

Attack Surface Management (day 6)

Scan the Attack Surface: The Cygienic platform scans your company's and critical vendor's domains across six critical checkpoints: email security, web security, vulnerabilities, data privacy, compromised systems, and open ports. You can view the scan results in "My Company Assessments" or "Admin Panel Reports" – results in hours, not days.

Attack Surface Report: results are crucial for understanding your company's perimeter or attack surface. An 'A' grade indicates a strong security posture, whilst an 'E' grade signifies poor security and vulnerability to cyberattacks. The report will also provide remediation guidelines, planning tools, and costs.

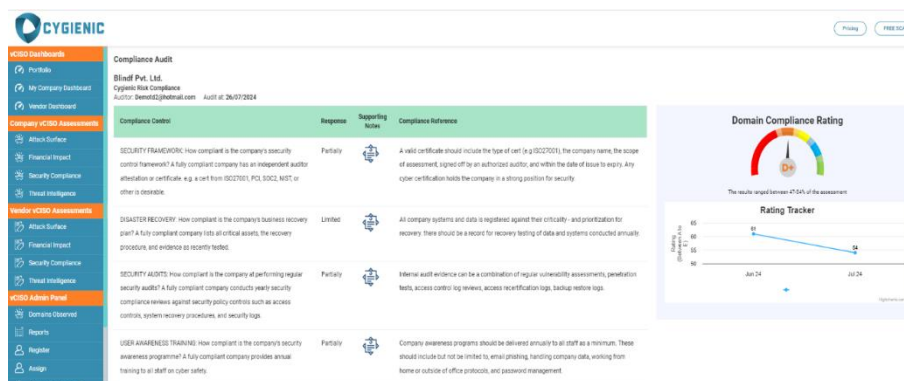
Schedule Attack Surface Scans: Scans can be scheduled daily, weekly, or monthly, and you can opt to receive the reports via email.



Security Compliance Assessment (day 7)

Perform Compliance Assessment: Assess the potential impact of your company's compliance controls against the proprietary Cygienic Risk Compliance questionnaire. Completing this assessment should take no more than a few hours.

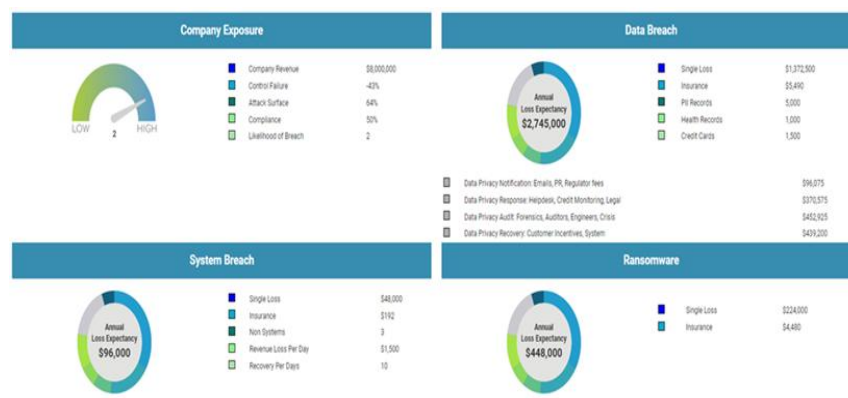
Security Compliance Report: results are crucial for understanding your company's compliance. An 'A' grade indicates a strong security posture, whilst an 'E' grade signifies poor security and vulnerability to cyberattacks. The report will also provide remediation guidelines, policies, planning tools, and costs.



Financial Risk Analysis (day 8)

The Cygienic platform offers a clear and comprehensive measurement of potential risk versus return on investment. It helps calculate cyber insurance premiums, costs of data breaches, and ransomware impacts, building your financial risk profile. This enables more informed cybersecurity investment decisions. By completing the 'Financial Audit' module, the platform's algorithms will generate your financial impact assessment.

- Data Breach cost analysis
- Ransomware cost analysis
- Business Interruption cost analysis
- Cyber Insurance cost analysis



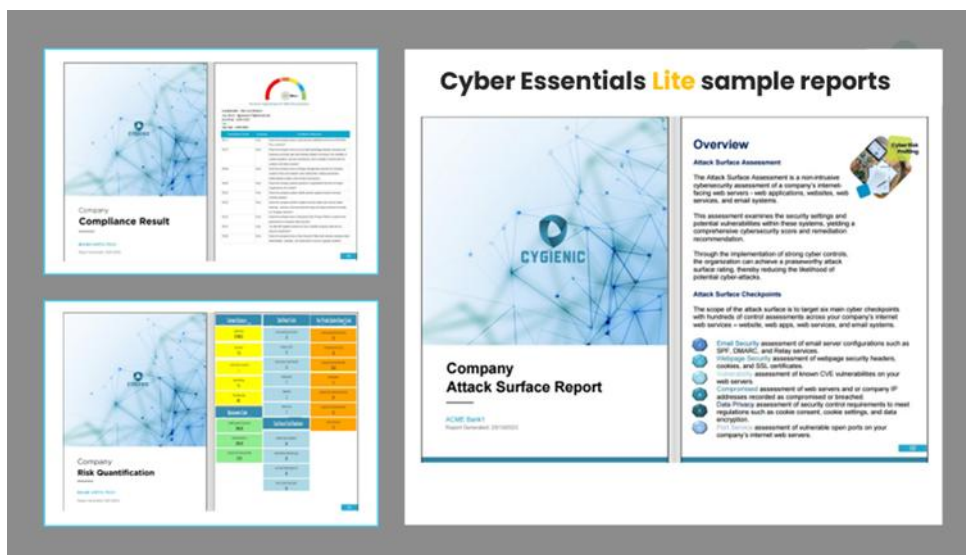
Threat Intelligence Analysis (days 9-10)

Gathering Threat Intelligence couldn't be easier. Cygienic offers a user-friendly search and discovery toolbox to detect data leaks, email credential leaks, threat adversaries, and performs vulnerability and compromised server scans. This simplified, pre-configured executable search toolbox delivers immediate results with no expertise or configuration required. Build a threat profile in a day, not a week.

- Cyber Threat Analysis
- Deepweb data discovery
- Code repository data discovery
- Google Public share data discovery
- Paste sites data discovery
- Company server data discovery
- Email credential breach check
- Vulnerability server scanners
- Compromised server scanners

Communicate Findings via Executive Summary Reports (day 10)

Cyber Risk Reports: Present a comprehensive summary of your initial findings to the executive team, emphasizing key risks, immediate concerns, and areas requiring attention. Access over 25 professional cyber risk management reports through the 'Admin Panel Reports'.



Days 11-13: Developing the Strategy & Thresholds

Define Cybersecurity Objectives (days 11-12)

Alignment with Business Goals: Ensure your cybersecurity objectives align with the overall business goals and strategies.

Short-term and Long-term Goals: Set clear, measurable short-term and long-term cybersecurity goals.

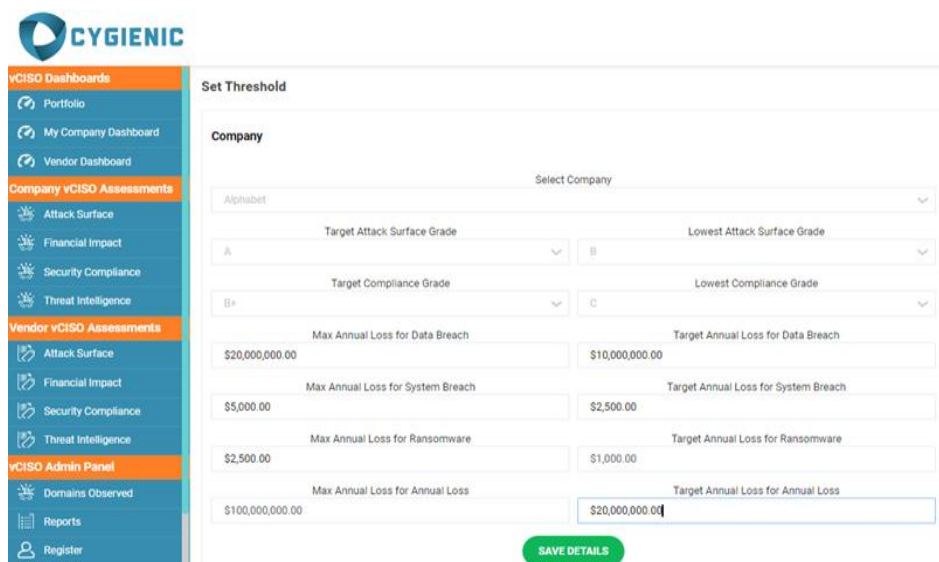
Strategic Vision: Develop a long-term vision for cybersecurity within the organization. Ensure it aligns with the company's future goals and growth plans.

Leadership Role: Solidify your role as a leader in the organization. Continue to build trust and demonstrate your commitment to protecting the organization's assets.

Set Targets and Thresholds KPIs (day 13)

Key Performance Indicators (KPIs): Establish KPIs to track the progress of your cybersecurity initiatives- use progress and set thresholds & targets for finances, compliance levels, and grades via the 'Cygienic Threshold Mgmt.' module.

Regular Reviews: Conduct regular reviews to assess the effectiveness of implemented measures and adjust strategies as needed.



The screenshot displays the Cygienic vCISO Admin Panel interface. On the left is a navigation sidebar with sections: vCISO Dashboards (Portfolio, My Company Dashboard, Vendor Dashboard), Company vCISO Assessments (Attack Surface, Financial Impact, Security Compliance, Threat Intelligence), Vendor vCISO Assessments (Attack Surface, Financial Impact, Security Compliance, Threat Intelligence), and vCISO Admin Panel (Domains Observed, Reports, Register). The main content area is titled 'Set Threshold' and contains a form for configuring thresholds for a selected company (currently 'Alphabet'). The form includes dropdown menus for 'Target Attack Surface Grade' (set to 'A') and 'Lowest Attack Surface Grade' (set to 'B'), 'Target Compliance Grade' (set to 'B+') and 'Lowest Compliance Grade' (set to 'C'). Below these are input fields for 'Max Annual Loss' and 'Target Annual Loss' for three categories: Data Breach (\$20,000,000.00 / \$10,000,000.00), System Breach (\$5,000.00 / \$2,500.00), and Ransomware (\$2,500.00 / \$1,000.00). A final row for 'Annual Loss' shows a Max Annual Loss of \$100,000,000.00 and a Target Annual Loss of \$20,000,000.00. A green 'SAVE DETAILS' button is located at the bottom right of the form.

Days 14-17 Remediation Planning

Remediation Planning (days 14-17)

Prioritize Initiatives: Rank security initiatives based on risk assessment findings and business needs. Track all Attack Surface and Security Compliance assessments against remediation plans, risk priorities, timelines, and costs, via Cygienic Assessment modules.

Resource Allocation: Identify necessary resources, personnel, and technology, to achieve your objectives via Cygienic Assessment modules.

Timeline & Costs: Create a realistic timeline for implementing security initiatives and achieving milestones and associated costs, via Cygienic Assessment modules

The screenshot displays the Cygienic Compliance Audit interface. On the left is a sidebar with navigation options: vCISO Dashboards, vCISO Assessments, vCISO Admin Panel, and vCISO Cyber Scanners. The main content area is titled 'Compliance Audit' and shows a table with columns for Recommendation, Result, Policy & Guides, and Response. The table contains three rows of data, each with a recommendation, a result status (e.g., Fully Compliant, Partially Compliant), and a response plan. A red vertical line separates the 'Policy & Guides' column from the 'Response' column. At the top right, there are buttons for 'Print' and 'Export'. A warning message at the top right states: 'Your responses are auto saved. You can click the "BACK" button to leave the page safely and your responses will be saved. Your guide updates are only submitted when you click "SAVE COMPLIANCE".'

Recommendation	Result	Policy & Guides	Response
It is the A fully auditor 1 estimate A valid certificate should include the type of cert (e.g. ISO27001), the company name, the scope of assessment, signed off for an authorized auditor, and within the date of issue to expiry. Any other certification notes the company in a strong position for security.	Fully Compliant	Accept	Accept
It is the By the the entity All company systems and data is registered against their criticality - and prioritization for recovery. There should be a record for recovery testing of data and systems conducted annually.	Partially Compliant	Accept	Accept
It is the By the the entity Internal audit evidence can be a combination of regular vulnerability assessments, penetration tests, access control log reviews, access recertification logs, backup-restore logs.	Partially Compliant	Accept	Accept

Days 18-20: Implementation & Continuous Monitoring

Initiate Quick Wins Projects (day 18)

Quick Wins: Focus on achieving some quick wins to build momentum and demonstrate the value of cybersecurity initiatives.

Long-term Projects: Start laying the groundwork for long-term projects that will require more time and resources.

Prepare for Continuous Improvement (day 18)

Feedback Loop: Create a feedback loop to continuously improve security practices based on lessons learned and evolving threats. By setting up Cygienic vCISO to continuously scan and send reports, you will be able to monitor any deviation and progress.

Ongoing Training: Ensure that ongoing training and development opportunities are available for your team to stay ahead of new threats and technologies.

Reflect and Adapt (day 19-20)

Review Achievements: Reflect on what you have accomplished in the first 18 days. Identify successes and areas for improvement.

Adjust Plans: Adapt your plans based on feedback and the evolving security landscape.

Prepare for Ongoing Challenges (day 19-20)

Stay Informed: Stay updated on the latest cybersecurity trends, threats, and technologies.

Continuous Improvement: Foster a culture of continuous improvement and resilience in your cybersecurity practices.

Conclusion

The first 20 days as a Hyper-performing vCISO are pivotal in setting the foundation for a successful tenure. By understanding the landscape, building relationships, developing a strategic roadmap, and implementing key initiatives, you can establish yourself as a trusted leader and protect your organization from evolving cyber threats. Remember, cybersecurity is a continuous journey, and your ability to adapt and lead will be crucial in navigating this dynamic field.

Getting Started with Cygienic vCISO

Overview of Cygienic.com Platform

Cygienic.com is a state-of-the-art cybersecurity risk management platform designed to help organizations identify, assess, and mitigate cybersecurity risks. It offers a suite of tools for cyber risk assessment, attack surface management, threat intelligence, financial risk management, and compliance management, providing a holistic approach to cybersecurity.

Accessing the Platform

To access Cygienic.com, navigate to the official website and click on the login button. Enter your credentials to access the dashboard.

Account Setup

To set up an account contact sales@cygienic.com

User Interface Overview

The user interface of Cygienic.com is designed to be intuitive and user-friendly. Familiarize yourself with the main sections:

Dashboard: Provides an overview of your organization's cybersecurity status.

Company Assessments: Tools and features for assessing and managing company attack surface, compliance, and financial risks.

Vendor Assessments: Tools and features for assessing vendors & managing company attack surface, compliance, and financial risks.

Admin Panel: Register companies, assign domains and users, query & reports.

Cyber Scanners: Live scanners for cyber ratings, vulnerability, data breach, email breach, IP address.

Cyber Library: Policies, technical documents, cybersecurity awareness.



Contact sales@cygienic.com to discuss our Cygienic subscription.