cynomi

Top virtual CISOs share: 7 top tips on how vCISO service providers can maximize services, increase revenues, and improve margins



Content

Introduction	3
Tip 1. Prepare to deliver	4
Tip 2. Know before you go	6
Tip 3. Understand compliance requirements	7
Tip 4. Devise a strategy and plan	8
Tip 5. Don’t diverge from the vCISO duties	10
Tip 6. Focus on SMEs	12
Tip 7 Use software to automate and scale your vCISO work	14
The AI-Powered, Automated vCISO Platform	16

Introduction

When you want advice on how to expand, who better to go to than the people who have been there, seen it, and done it with success. Accordingly, we interviewed some of the top virtual Chief Information Security Officers (vCISOs) around to find out their secrets. Some passed on some great tips that helped them maximize their ability to deliver top-notch service to their customers. Others focused on how to increase revenues and improve margins. And a couple zeroed in on what it really takes to scale up vCISO services effectively.

Gathered from the input of top vCISOs, here are the top 7 tips.





Tip 1
Prepare to deliver

"Never let vCISO appointments detract from ongoing MSP/MSSP service delivery efforts."

vCISO manager at a Florida-based MSSP

When seeking to expand vCISO service delivery to a wider range of customers, ensure that those delivering are capable of doing so competently. A vCISO should be experienced in the world of security. Many have degrees in IT or hold cybersecurity certifications. vCISO duties demand management and security expertise. This factor of experience is one of the factors that can make it challenging to deliver and scale vCISO services.



- **Maintain quality:** As the vCISO clientele list grows, tasks can't easily be handed off to other personnel. Any MSP doing so could endanger its reputation by using unqualified personnel to provide advice and strategy to customers. As you expand, pay attention to quality.
- **Be Smart:** Additional vCISO candidates chosen from within existing ranks are likely to already be overloaded. Don't rob Peter to pay Paul.
- **Train:** One solution is to train and certify internal resources to enable them to take over some of the functions.



Tip 2
Know before you go

"Without a thorough cybersecurity risk assessment, you are flying blind."

Independent cybersecurity consultant and vCISO

You can't protect what you don't understand. The bread and butter of the vCISO role is the risk assessment.

- **Assess:** The vCISO should focus on completing a thorough risk assessment and document the existing cybersecurity risk posture for every client.
- **Use Existing Frameworks:** Use the NIST Risk Management Framework, the Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Risk Assessment framework, the Factor Analysis of Information Risk (FAIR Risk), Threat Agent Risk Assessment (TARA), and others.
- **Assess Again:** Risk assessments must be regularly updated to keep pace with a constantly shifting risk profile.



Tip 3
Understand compliance requirements

"Make sure you carefully identify any and all rules and regulations that may apply."

Fractional CISO, NY-based MSP

Failure to comply with regulations can result in hefty fines that damage the bottom line. When publicly revealed, compliance violations can seriously damage reputation. In tandem with thorough cyber-risk assessments, vCISOs need to understand the compliance requirements of each client. These vary markedly from industry to industry and from region to region.

- **Do Your Homework:** There are many rules, standards, regulations, and codes to adhere to. Catalogue all applicable standards such as NIST, ISO 27001 etc., as well as applicable regulations such as HIPAA, GDPR, and others.
- **Augment Risk Assessments:** Some risk assessments concentrate only on vulnerabilities and potential threats. Be sure to include compliance risk as part of any risk assessment.



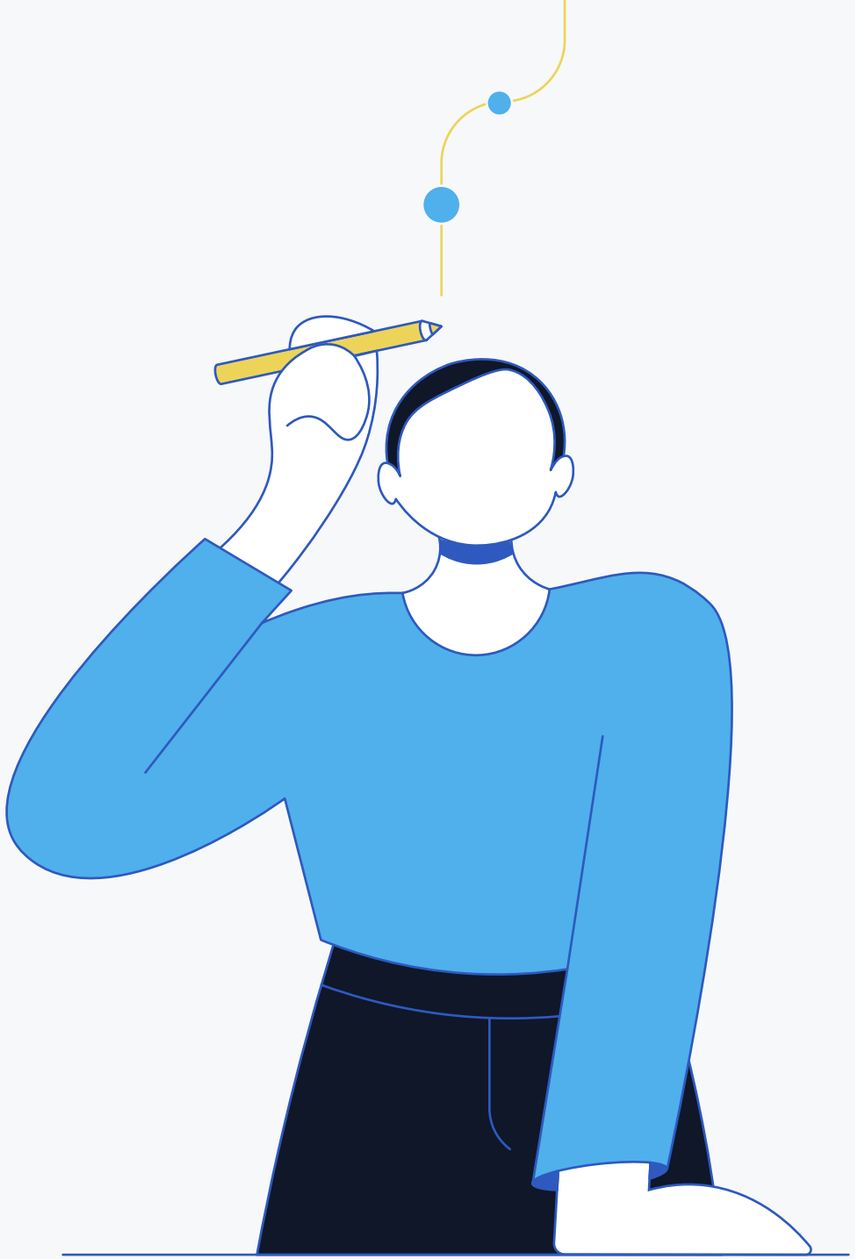
Tip 4

Devise a strategy and plan

"Strategic planning must be realistic and executable by existing resources."

vCISO team leader, Large professional services company, Indiana

Once a thorough risk assessment (and comprehensive compliance research) is done, it is up the vCISO to devise a strategy to guide the organization.



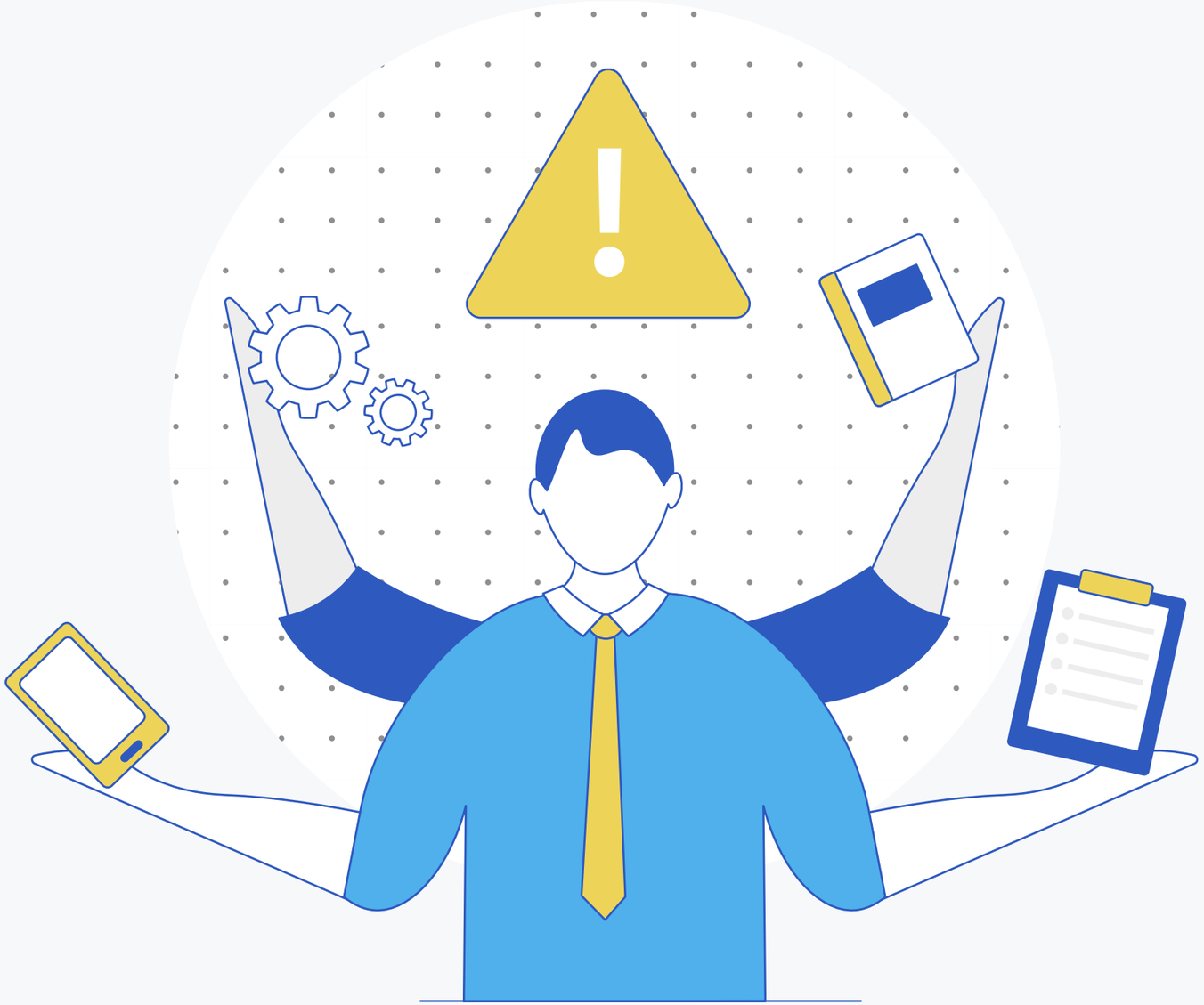
- **Planning:** Break the strategy down into an actionable and prioritized remediation plan that lays out the many steps that need to be taken by IT, security personnel, and others.
- **Policy:** The CISO develops and regularly revises security policies to address issues uncovered in assessments.
- **Procurement guidance:** The strategic plan guides all procurement activities. This is necessary to avoid reactive procurement practices that lead to bit-and-piece software and hardware acquisition.
- **Revise:** These plans are subject to regular revision as attack vectors and tactics shift. The organization's risk profile one month may be quite different a few weeks later.

Tip 5

Don’t diverge from the vCISO duties

“I demand that the customer’s IT and security staff contain the day-to-day noise while I assess the situation and devise strategy that leads to long-term resolution.”

vCISO at a cybersecurity consulting firm, California



Some inexperienced vCISOs get sucked into the everyday cybersecurity noise. It is a fatal error. The vCISO role comprises:

- **Cyberattacks:** Development and implementation of processes and systems used to prevent, detect, and mitigate cyberattacks.
- **Risk:** Monitoring, evaluating, and managing overall cybersecurity and technology risk in coordination with business leaders.
- **Strategy:** Setting an all-encompassing cybersecurity strategy that guides technology investment.
- **Compliance:** Overseeing cyber governance, risk, and compliance processes.
- **Reports:** Supplying top management and the board with comprehensive reports.
- **Execution:** Getting plans done via strong project management capabilities.

→ **Delegate:** vCISOs have no business becoming embroiled in the workaday world of cybersecurity or the resolution of the latest security situations. They can and should offer advice. But they should delegate to others to directly address these matters.

→ **Recommend MSP Services:** Top vCISOs help their clients by recommending further MSPs services (their own or from other MSPs) such as extended detection and remediation (EDR) and patch management.

Top vCISOs know when to pass the baton.

Tip 6
Focus on SMEs

"Hackers realize that SMEs often represent an easy target due to lack the resources, security expertise, and enterprise-class security tools."

Independent CISO-as-a-Service consultant, Washington

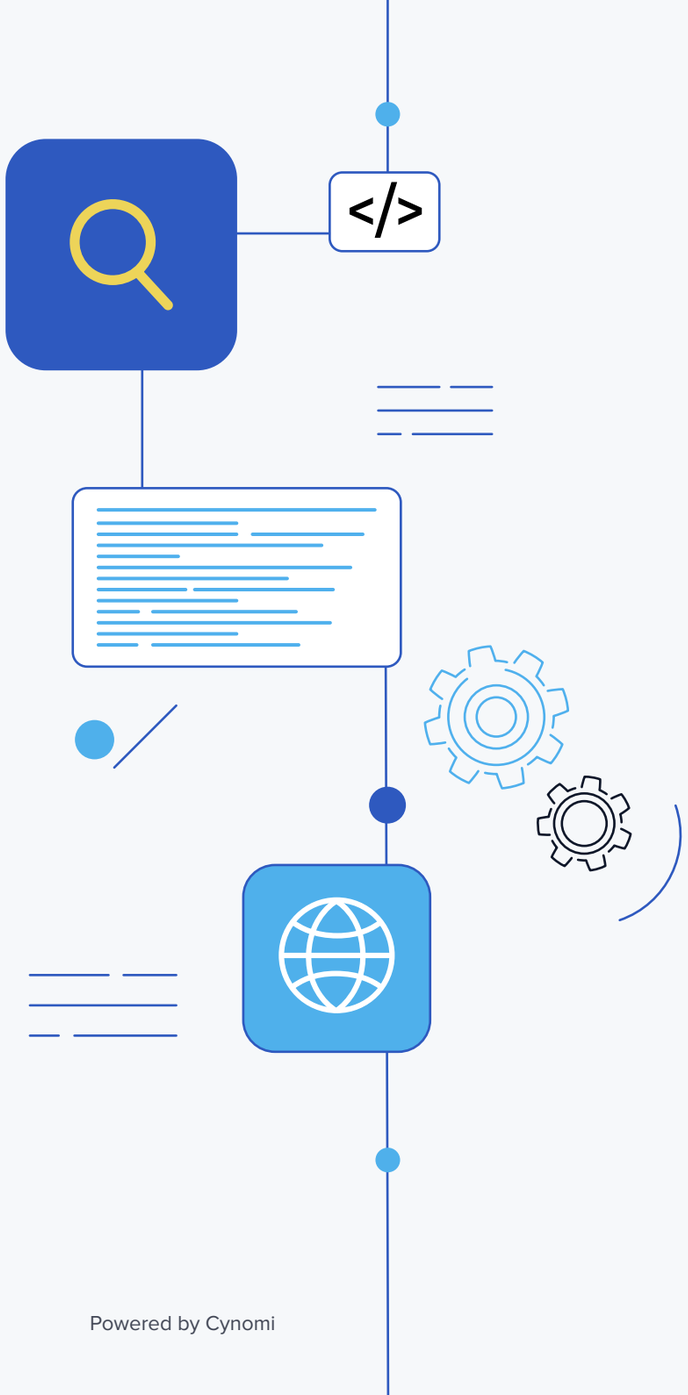
SMEs are dealing with an increase in the volume and sophistication of attacks. At the same time, they are facing increasing compliance requirements and regulatory scrutiny. When they turn to cybersecurity insurance providers for help, they are being told to implement sophisticated and expensive cybersecurity systems that are often beyond their level of technical competence.



- **Market to SMEs:** Due to factors such as attack volume, regulatory pressure, and the demands of cyber-insurance providers, SMEs need vCISO services more than ever. Focus your marketing efforts on SMEs.
- **Cost Containment:** Skilled CISOs are difficult to find. Even if candidates are available, few SMEs can afford them due to the high salaries demanded. Top vCISOs know they bring affordable C-level assistance to SMEs that prevents breaches, reduces risk, and mitigates the consequences of attacks.
- **Low-Hanging Fruit:** Some states require by law that organizations in certain industries fill the CISO position. SMEs operating in financial services, for example, can fulfill this requirement by hiring a vCISO.

SMEs desperately need a vCISO. This represents the richest and ripest area of service potential.





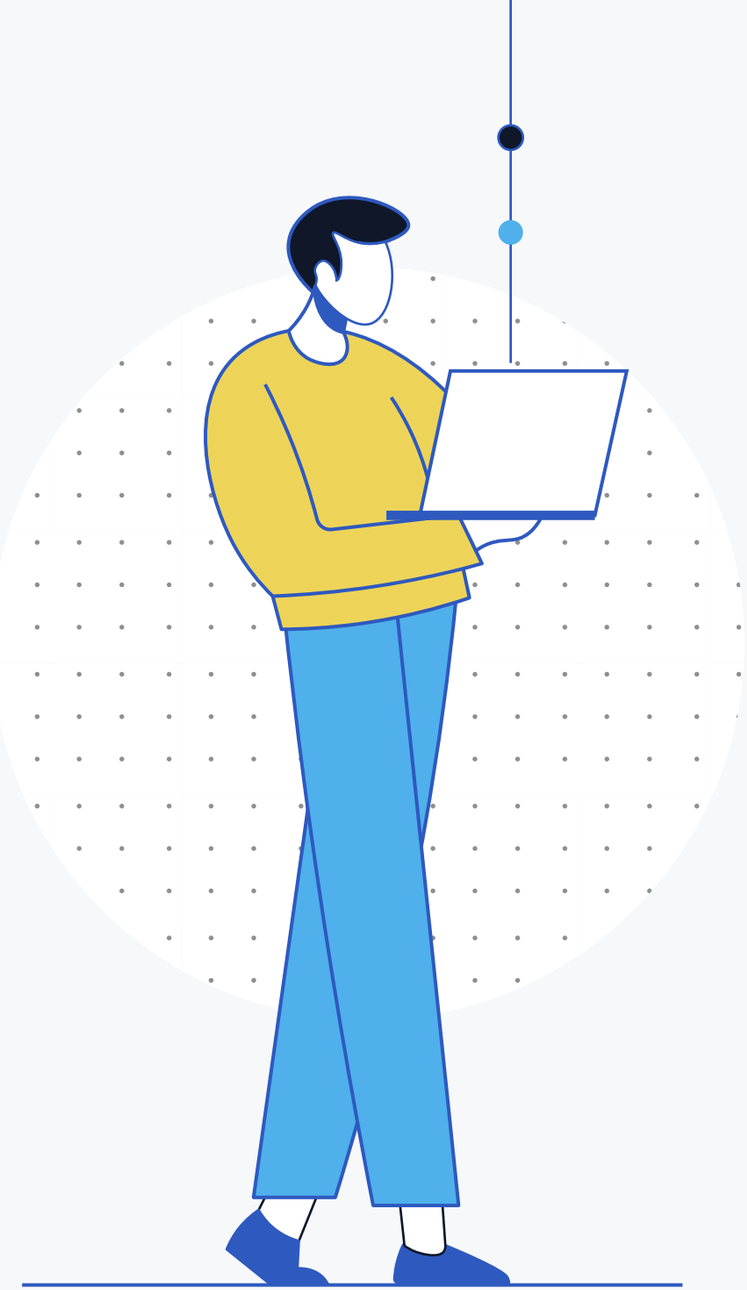
Tip 7

Use software to automate and scale your vCISO work

"Implementing a vCISO platform, has helped us scale work without scaling in-house resources"

MSPs delivering vCISO services love their high-margin potential. Good margins can be maintained for a few clients. Beyond that, vCISO services are difficult to scale. Due to factors such as:

- Lack of trained vCISO-class personnel resources is a major barrier to service scalability.
- The vCISO position is time consuming. They must constantly be on the alert, stay on top of ever-shifting risk profiles, and must dig into the details of risk assessment and cybersecurity planning while staying on top of compliance and execution.
- Once a certain threshold is passed, vCISOs become overloaded. Bottlenecks occur and quality of service suffers. That's when margins slip.



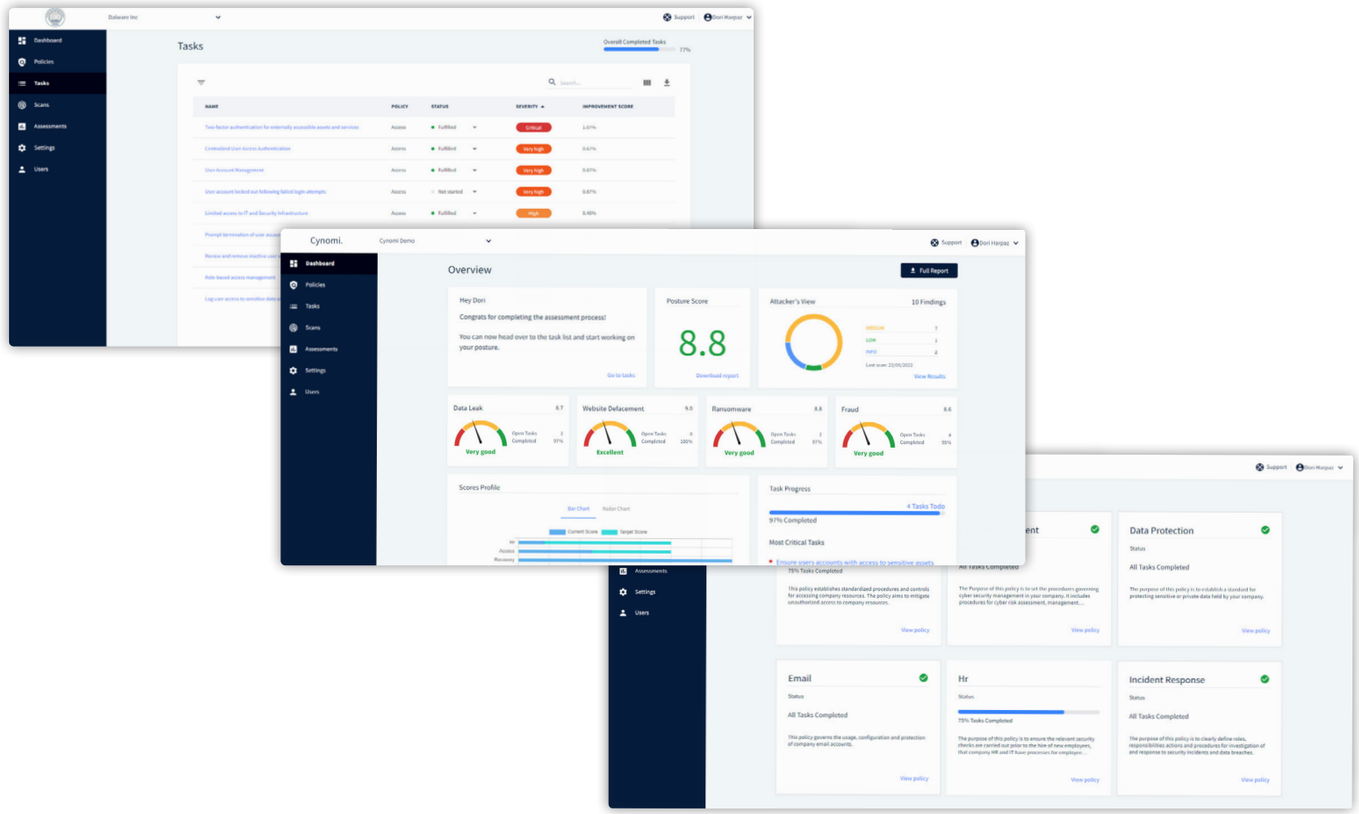
Adopt vCISO Platforms: vCISO platforms are available that combine automation with Artificial Intelligence (AI) to automate risk and compliance assessments, auto-generate tailored policies, and provide actional remediation plans with detailed priorities, task management tools, progress tracking, and customer facing reports. This is accomplished by modeling AI algorithms on the best practices adopted by the world's best vCISOs and CISOs. These platforms eliminate much of the labor absorbed in manually assessing risk, scrolling laboriously through logs, and being bogged down in time-consuming processes. The best ones can even assist service providers to bridge the vCISO skills gap.

Top vCISOs use vCISO platforms to be able to scale up effectively while maintaining high margins.

"My vCISO platform takes care of the most time-consuming aspects of risk assessment, general planning, compliance, and tracking of execution automatically, allowing me to deliver effectively to a greater volume of customers."

The AI-Powered, Automated vCISO Platform

Cynomi's multitenant platform automatically generates everything needed to provide vCISO services at scale: Risk and compliance assessments, gap analysis, tailored policies, strategic remediation plans with prioritized tasks, tools for ongoing task management, progress tracking and customer-facing reports.



Tailored security policies

Easy-to-follow, actionable security policies, based on your client's cyber profile, relevant regulatory requirements and industry benchmarks.

Prioritized remediation plan and tasks

A customized, prioritized, remediation task list for each client, with impact and criticality rate for each task. Tasks are completely editable.

Customer-facing reports

Exportable customer-facing status and progress reports with your brand, for customer stakeholders - operations and management alike.

Ongoing task management and progress tracking

Ongoing remediation task management, collaboration and progress tracking tools.

Vulnerability and exploit gap analysis

Illuminates the vulnerabilities to which each client is exposed and prioritizes remediation steps.

Full multi tenancy

Create and manage accounts for each of your clients from a single dashboard, and manage access and roles for each client.

For more information, visit: www.cynomi.com