CISO GLOBAL

COURSE CATALOG

Empower Your Employees or Advance Your Career
Through Expert Led Training With CISO Global

For more information, please contact us
480-389-3444 or visit www.ciso.inc

CYBER DEFENSE TRAINING

What Is Cyber Defense Training?

Our cyber defense training courses teach the skills you need to combat the cyber threats you face today—and emerging threats you will face tomorrow. Topics include computer and network exploitation methodologies, packet analysis, network traffic analysis, malware forensics, malware analysis, and reverse engineering malware. We also introduce programming and scripting concepts in languages such as Python, Java, C++, and C# that are fundamental in malware analysis, reverse engineering, and digital forensics.

Why Choose CISO Global?

Our trainers are highly skilled industry veterans with decades of experience working in the cybersecurity and IT fields. They hold the most important cybersecurity-related certifications, including those from (ISC)2 and CompTIA. They have taught in-person and online, delivering cybersecurity training to corporate, military, government, and higher education students. You receive hands-on training with relevant industry tools and techniques that incorporate real-life cyber threat scenarios, so you can detect, diagnose, and mitigate a range of exploits and attacks.

Our cyber defense training program stands out because of our approach:

- Our trainers bring with them decades of cybersecurity expertise combating many cyber threats as well as years of training others to do the same.
- You will train using the same tools and techniques you use to fight the cyber threats your organization is likely to face.
- Course content is engaging, challenging, constantly updated, and relevant to current and emerging cyber threats.

Professional–Grade Cyber Defense **Skills Training**

CISO GLOBAL

480-389-3444 | ciso.inc

CISO Global Teaches These Cyber Defense Skills

Computer and Network Exploitation Methodologies (1 day)

This course provides you with an overview of penetration testing, red teaming, vulnerability analysis, and exploitation methods that you practice using directed hands-on exercises.

Packet Analysis (1 day)

This course teaches you the fundamental concepts, methodologies, and tools necessary to analyze network traffic for the purposes of intrusion and threat detection, network defense, and low-profile offensive operations. The course begins with an introduction of the role of network packet analysis in computer network operations and progresses to a detailed discussion of the TCP/IP protocol suite and ethernet network operations. You will practice using a protocol analyzer to capture and analyze self-generated network traffic. You will learn how to examine packet captures, which illustrate various exploits, network reconnaissance techniques, and more advanced network attacks.

Network Traffic Analysis (5 days)

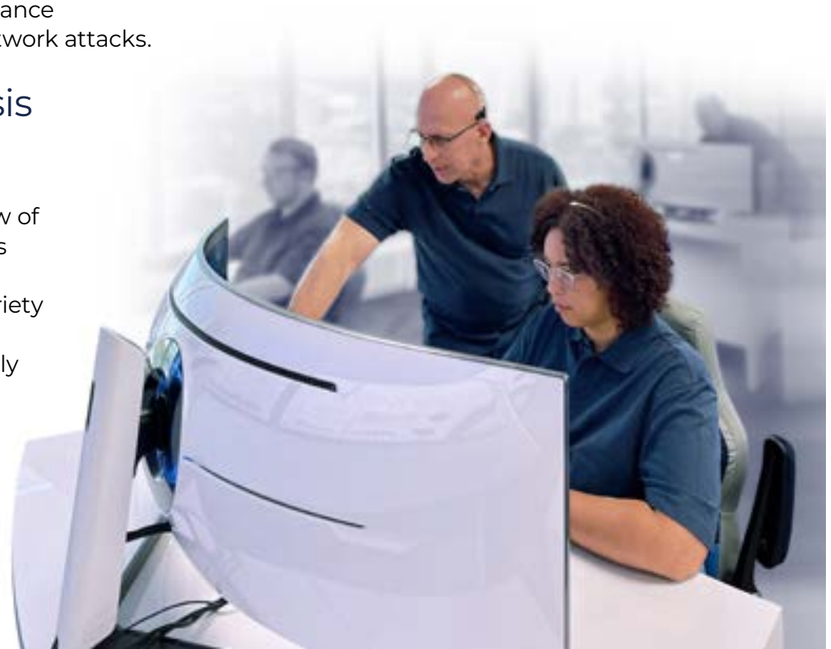
This course provides you an overview of best practices in analyzing malicious network traffic. You will acquire a fundamental understanding of a variety of network-based malware analysis tools and techniques that can directly support your organization's incident response efforts and increase your performance in your functional role(s). You will be given real-world packet capture samples to dissect in a controlled environment.

Malware Forensics (5 days)

This course teaches you the fundamental requirements necessary to analyze malicious software from a behavioral perspective. You will observe malware in a controlled environment using system monitoring tools to analyze malicious affects to systems. You will analyze a wide variety of current threats, from simple keyloggers to massive botnets, using real-world samples. Survey level – no experience in coding required.

Basic Malware Analysis (5 days)

This course teaches you the fundamentals of analyzing malicious code. It focuses on static malware analysis and touches on dynamic malware analysis. Dissect real-world malicious code samples in a controlled environment. Beginner level – some coding experience recommended. View additional courses in coding/programming.



Intermediate Malware Analysis (4 days)

Building on Basic Malware Analysis, this course focuses on dynamic malware analysis using three critical tools for successful malware analysis: disassemblers, decompilers, and Windows SysInternals. You will identify host-based and network-based indicators of compromise and Windows APIs often used by malware authors. You will be given real-world malicious code samples to dissect in a controlled environment. Intermediate level – completing our Basic Malware Analysis course and some coding experience recommended. View the options below for courses in coding/programming.

Reverse Engineering Malware (5 days)

Building on Intermediate Malware Analysis, this course dives deeper into performing dynamic malware analysis using a debugger. You will learn how to identify exactly what a malware sample does and how it does it. You will learn how to patch the sample to make sections inactive or crack the program to allow full access to areas hidden or encrypted by the malware author. You will be given real-world malicious code samples to dissect in a controlled environment. Intermediate level – completing our Intermediate Malware Analysis course and some coding experience recommended. View the options below for courses in coding/programming.

Regular Expressions (1 day)

This course teaches you how to use regular expressions to search through larger collections of data quickly and efficiently.

Burp Suite Pro (2 days)

This course teaches you how to use the popular vulnerability scanning tool Burp Suite Pro that enables you to easily find vulnerabilities in web applications. You will also be exposed to the differences between Burp Suite's Community Edition and Professional (Pro) Edition.

Introduction to Python Scripting (2 days)

This course introduces you to Python scripting, a popular language used in cybersecurity. You will do practical exercises that teach you the aspects of scripting in this language. Topics include data types, operators, collections, external modules, functions, error handling, and analyzing data files. Hackers and penetration testers often use Python scripts in their activities. No previous experience with programming languages is required.

Introduction to Java Programming (5 days)

This course introduces you to Java programming language and software development problem-solving methodologies using current software design and development tools and techniques. Topics include data structures, program design, language control structures, procedures and functions, error handling, and object-oriented design using classes and inheritance. Hands-on exercises are developed in Java using a current integrated development environment (IDE). Learning a programming language is fundamental in performing malware analysis and reverse engineering. No previous experience with programming languages is required.

CISO GLOBAL

480-389-3444 | ciso.inc

CMMC TRAINING

Cybersecurity Maturity Model Certification Training

What Is a Certified CMMC-AB Licensed Training Provider?

The Cybersecurity Maturity Model Certification-Accreditation Body (CMMC-AB) established an approved Licensed Training Providers (LTPs) network of Provisional Instructors (PIs) to deliver training to those who want to obtain Certified CMMC Professional and/or Certified CMMC Assessor certifications.

Why Choose CISO Global?

CISO Global is a certified CMMC-AB LTP. The CMMC-AB considers only training provided by LPTs as valid for preparing for the CMMC-AB certifications. Our instructors are CMMC-AB certified PIs. They were required to go through a rigorous training process, followed by passing knowledge-based and performance-based examinations. This also included completing aggressive Provisional Assessor training to gain comprehensive knowledge about the CMMC Framework, validated by passing the certification examination. Additionally, they bring decades of experience in assessment and training.

We are currently scheduling the following classes:

Certified CMMC Professional Training (5 days)

A five-day course designed to prepare aspiring CMMC assessors for Cyber AB's Certified CMMC Professional examination. This course covers the CMMC model, the assessment guides, and how to interpret the CMMC model. An accredited LLP provides all course materials, as required by Cyber AB. **Students must take this course to be eligible to take the CMMC Certified Professional Examination.**

Certified CMMC Assessor Training (5 days)

A five-day course designed to prepare aspiring CMMC assessors for CyberAB's Certified CMMC Assessor examination. This course takes a more in-depth look into the CMMC model, the assessment guides, and how to interpret the CMMC model. It also takes an in-depth look at the CMMC Assessment Process (CAP) and the 110 security controls required under NIST SP 800-171 revision 2 required to be implemented for CMMC Level 2 Certification. An accredited LLP provides all course materials, as required by Cyber AB. **Students must take this course to be eligible to take the CMMC Certified Assessment Examination.**
Pre-requisite: Passing the CMMC Certified Professional (CCP) Examination.

CYBERSECURITY MATURITY MODEL CERTIFICATION

CISO GLOBAL

480-389-3444 | ciso.inc

CERTIFICATION TRAINING

Certification Training

Preparing for a certification assessment is a challenging task. Our certification training courses prepare you for taking – and passing – the most important cybersecurity certificate assessments. They include detailed reviews of the knowledge requirements, in-depth Q&A sessions, and sample questions from actual exams.

Why Choose CISO Global?

Our trainers are highly skilled industry veterans with decades of experience working in the cybersecurity and IT fields. They hold the most important cybersecurity-related certifications, including those from (ISC)2 and CompTIA. They have taught in-person and online, delivering cybersecurity training to corporate, military, government, and higher education students.

Our Certification Training program stands out because of our approach:

- Our trainers bring with them decades of cybersecurity expertise combating every type of cyber threat as well as years of training others to do the same.
- You will learn how to perfect your understanding of the concepts as well as how to take and pass the exam on your first attempt.
- Course content is engaging, challenging, constantly updated, and relevant to current certification requirements.

CISO Global Prepares You for These Certifications

(ISC)2 CISSP Certification Boot Camp (5 days)

The vendor-neutral Certified Information Systems Security Professional (CISSP) certification is the ideal credential for those with proven deep technical and managerial competence, skills, experience, and credibility to design, engineer, implement, and manage their organization's overall information security program to protect against sophisticated attacks. This course aids in preparation for the CISSP examination.

(ISC)2 CGRC (formerly CAP) Certification Boot Camp (5 days)

The vendor-neutral Certified in Governance, Risk, and Compliance (CGRC) certification course is ideal for IT, information security and information assurance practitioners who work in Governance, Risk and Compliance (GRC) roles and need to understand, apply, and/ or implement a risk management program for IT systems within an organization. This course aids in preparation for the CGRC examination.

(ISC)2 CSSLP Certification Boot Camp (5 days)

The vendor-neutral Certified Secure Software Lifecycle (CSSLP) certification course is ideal for Software Developers who are interested in making the code they write more secure with fewer vulnerabilities. It guides the Software Developer through the various stages of the Software Development Lifecycle (SDLC) providing insight into vulnerabilities and how to 'bake in' security throughout. This course aids in preparation for the CSSLP examination.

CompTIA Linux+ Certification Boot Camp (5 days)

This course covers common tasks in major distributions of Linux, including the Linux command line, basic maintenance, installing and configuring workstations, and networking in preparation for the CompTIA Linux+ Certification.

CompTIA Network+ Certification Boot Camp (5 days)

This course is intended for entry-level computer support professionals with a basic knowledge of computer hardware, software, and operating systems who wish to increase their knowledge and understanding of networking concepts and acquire the required skills to prepare for a career in network support or administration with the CompTIA Network+ certification.

CompTIA Security+ Certification Boot Camp (5 days)

This course is targeted toward the IT professional who has networking and administrative skills in Windows®-based Transmission Control Protocol/Internet Protocol (TCP/IP) networks and familiarity with other operating systems, such as Mac OS X®, Unix, or Linux. Ideal for those who wish to further their career in IT by acquiring foundational knowledge of security topics, prepare for the CompTIA Security+ certification examination, or use Security+ as the foundation for advanced security certifications or career roles.

CompTIA CySA+ Certification Boot Camp (5 days)

Cyber threats are increasing at an alarming rate every year and organizations' ability to defend themselves against full-scale distributed attacks quickly and effectively is becoming more and more difficult. This course is taught by leaders in network defense who work in the computer security industry, this course demonstrates how to defend large scale network infrastructure by building and maintaining intrusion-detection systems, network security auditing, and incident response techniques. You will learn how to isolate and prioritize threats in real-time. This course aids in preparation for the CompTIA Cybersecurity Analyst (CySA+) certification.

CompTIA PenTest+ Certification Boot Camp (5 days)

This course examines offensive hacking techniques as a step-in understanding Network Defense. This process is explored using a Penetration Testing framework and uses current hacking tools and techniques. During the course, simple but effective countermeasures are offered as steps in improving the Network Defense of the target. This course aids in preparation for the CompTIA PenTest+ certification.

CISO GLOBAL
480-389-3444 | ciso.inc

CUSTOM CYBERSECURITY AWARENESS TRAINING

The Best Protection Is a Culture of Awareness

What Is Awareness Training?

Cybersecurity Is every employee's responsibility. Human error is the #1 point of entry for data loss and compromises to critical infrastructure. Awareness training should be the cornerstone of your cybersecurity program, providing the fundamentals of cyber hygiene, demonstrating what not to do.

Why Choose CISO Global?

CISO trainers are experts on the latest cyberthreats. They know what It takes to educate staff at all levels to recognize and avoid them. They employ the latest tools and use real-world scenarios to test employees' ability to detect scammers. This includes training on unsolicited emails with links and attachments commonly referred to as 'phishing emails' and more advanced social engineering efforts that even the most careful employees could easily fall victim to.

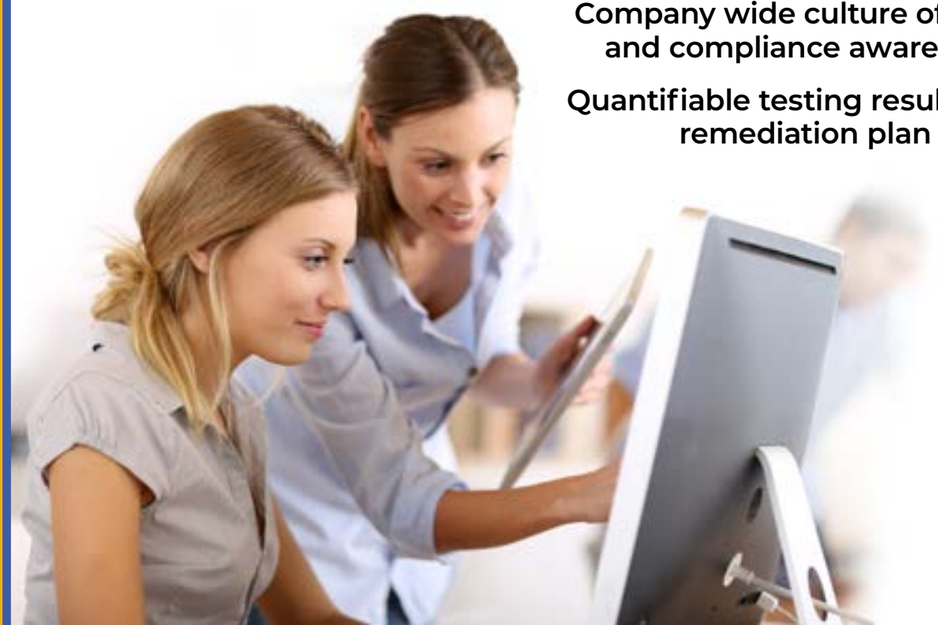
Our Awareness Training program stands out because of our approach:

- Awareness training program designed with real-life scenarios personalized to your industry
- Training materials on subjects such as social media scams and threats; handling sensitive information; privileged user training; and safe traveling best practices
- Personalized remediation plan with steps you can take to eliminate your weaknesses
- In-house team of remediation experts who can implement your personal plan

Key Program Outcomes

Company wide culture of cyber and compliance awareness

Quantifiable testing results with remediation plan



How CISO Global Creates a Culture of Awareness

Board-Level Buy-In

It's crucial you get Board-level buy-In on establishing and continuing a comprehensive, company-wide awareness training program as part of your risk management plan. Lack of employee security training can lead to costly ransomware attacks or other data breaches that can bankrupt or financially cripple an organization, damage Its reputation, and lead to legal troubles.

C-Suite–Level Education

Educating the C-suite on the importance of including awareness training as part of their overall risk management program through an understanding that it is foundational to effectively meeting their business needs.

An effective, ongoing company-wide training program can reduce costs, improve compliance, and boost morale by turning areas of uncertainty and anxiety into areas of strength.

Company-Wide Training

It is widely accepted that the human element Is the weakest link in every company's cybersecurity. The good news is that an educated workforce, everyone from newest Intern to experienced CEO, can become part of a new culture of awareness. Our targeted awareness training provides personalized modules that target the specific knowledge each level needs in order to quickly recognize and report phishing attempts and other malicious attacks.

CISO GLOBAL

480-389-3444 | ciso.inc

MANAGED CYBERSECURITY AWARENESS TRAINING

Managed Cybersecurity Awareness Training

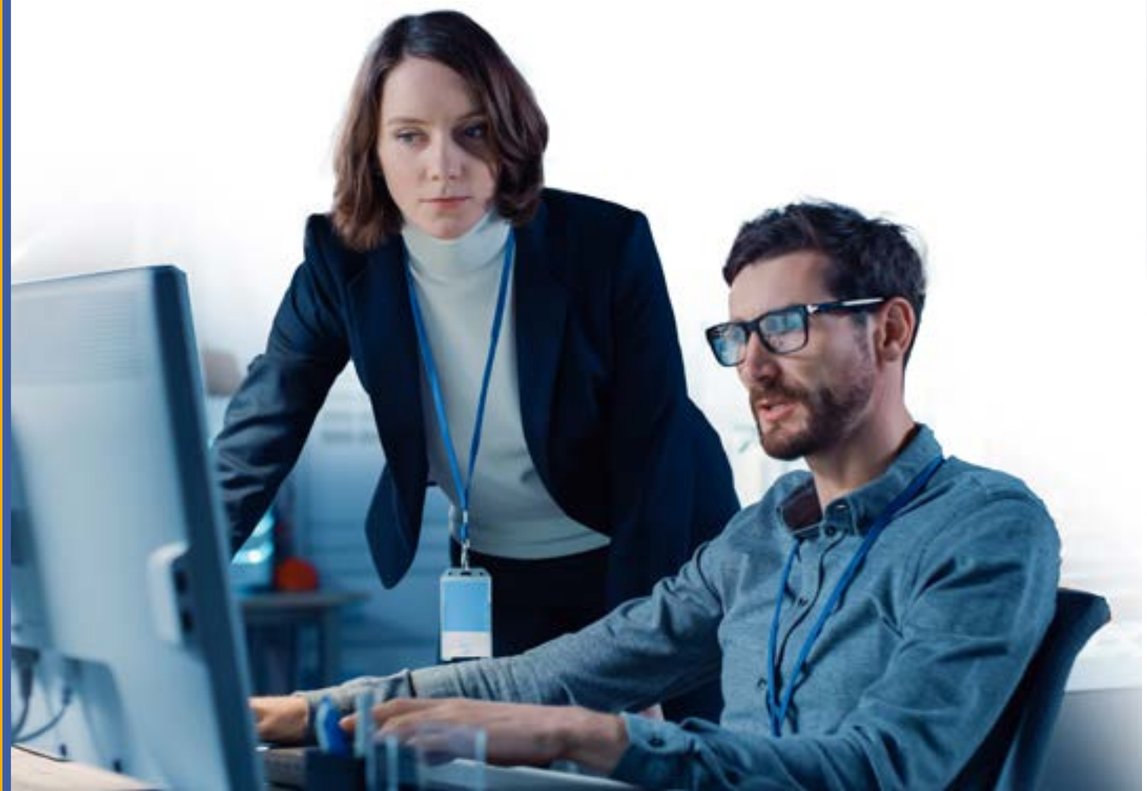
Providing Cybersecurity Awareness Training to your teams is required under most compliance frameworks, and recommended as a best practice under NIST standards, to help reduce your risk of a successful cyber-attack.

Content Overload

Many organizations choose to meet this requirement by purchasing a subscription-based service like KnowBe4 that gives access to over 1200 pieces of training content, as well as a simulated phishing campaign feature. It's easy to buy and fairly cost-effective, so why doesn't every organization use it? Most subscriptions are not renewed, because people find they lack the time needed to properly curate that much content.

Ineffective Phishing Campaigns

Further, if you want to know how well your teams can spot a real phishing email, you'll need the most robust subscription, and you'll want to invest time into learning how to customize emails to look legitimate. Otherwise, emails are too obvious, so they don't measure or teach prevention skills.



With CISO Global, you'll get:

Customized Learning Tracks

- Monthly security awareness training emails with curated content, tailored to your organization's training needs.
- Our experts are very familiar with KnowBe4 content and will hand-select the most effective modules for your team.
- Concepts are designed to build on one another.

Quarterly Reporting

- Our team will provide you with metrics on both progress and improvement over time.
- You'll always know where your teams stand.

Additional Training Services:

- Training for every level of your team:
- Live, custom training from one of our experts can address gaps and increase engagement.
- Narrated slide shows (with subtitles) on your organizational templates that you can save and re-use.
- Cybersecurity training for IT leaders – empower your leadership with advanced cybersecurity training.
- Cybersecurity Escape Room – CISO experts will set up a live, gamified escape room experience in your building to reinforce basic cybersecurity skills. Highly interactive and can be set up as a competition or raffle.

CISO GLOBAL

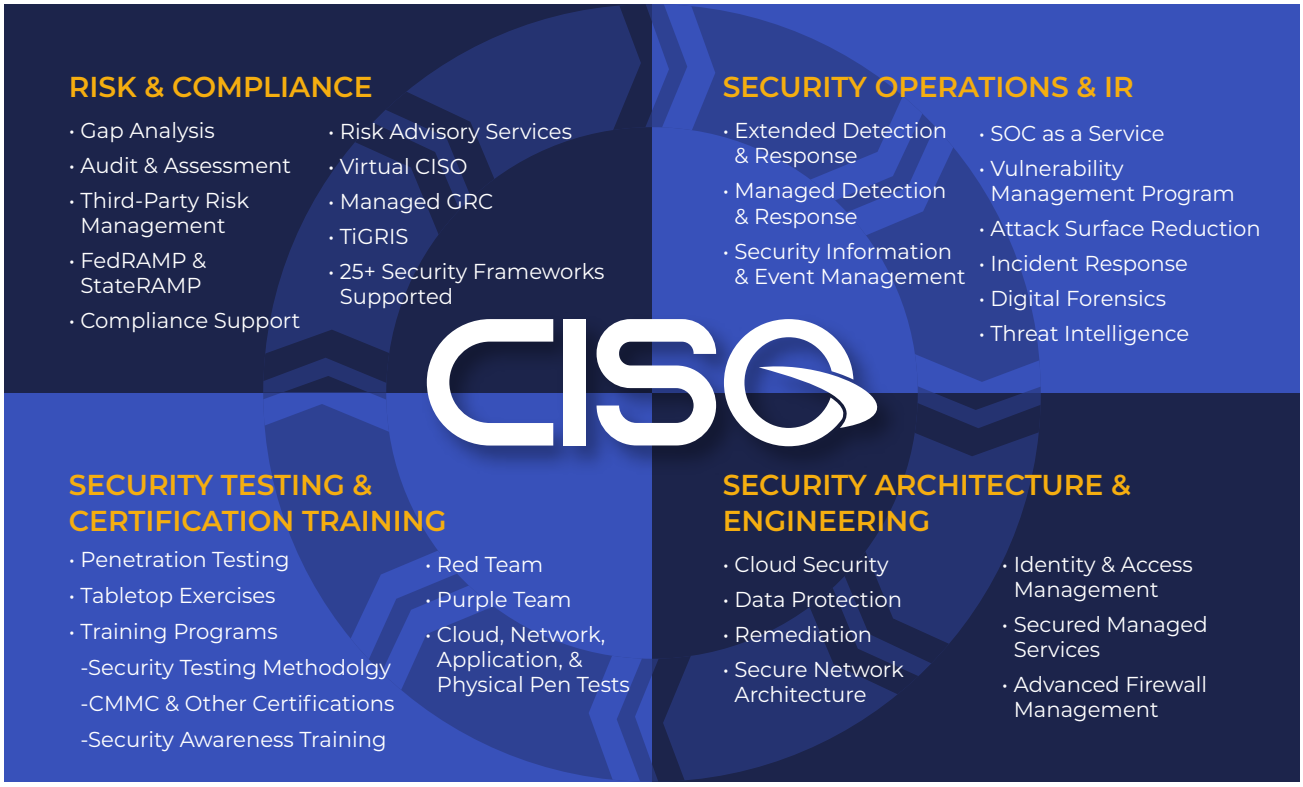
480-389-3444 | ciso.inc

ABOUT CISO GLOBAL

About Us

A leader in cybersecurity and compliance services, CISO Global brings together expert practitioners and thought leaders to provide tailored solutions that drive cyber resilience. The company's top-tier talent spans geographies, specialties, industries, regulatory frameworks, and focus areas and includes auditors, compliance specialists, certified forensics experts, ethical hackers, security engineers, and around-the-clock analysts.

To learn more, visit www.ciso.inc.



AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
SOC 2® Type II Audited

CISO GLOBAL

480-389-3444 | ciso.inc