CyberEd.io

Cybersecurity Education, News & Insights • Fall 2023

Perceptions versus reality:

Survey highlights need for more and better training

p. 16

Overcoming the Inertia of Assessing and Securing APIs

A conversation with Richard Bird

p. 10

Richard Bird
Chief Security Officer
Traceable AI

ISMG

70% of cybersecurity leaders say they don't have enough skilled cybersecurity employees.

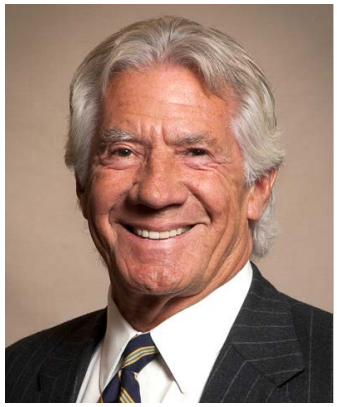
LET'S GET SMARTER.

CyberEd.io is reinventing conventional security awareness with continual learning. Our course library is rich with relevant content for C-suite execs, CISOs, senior practitioners, entry-level employees, and staff typically not involved with cybersecurity in their daily job duties. We build Cyber-Warriors at every level.

CyberEd.io

375.456.3350 | Cybered.io | info@cybered.io

Letter from the Senior Vice President



Steve King
Senior Vice President,
CyberEd.io

An experienced cybersecurity professional, Steve has served in senior leadership roles in technology development for the past 19 years. He has founded three Cybersecurity startups with successful exits, and has served as the CISO for Wells Fargo Bank's Global Retail technology division. He also served as CIO for Memorex and was the co-founder of the Cambridge Systems Group.

Welcome to CyberEd Magazine's Fall 2023 issue

CyberEd magazine is published quarterly to promote our relaunch of CyberED.io, the cybersecurity education division of Information Security Media Group. This Fall 2023 issue of our magazine is designed to offer worthwhile intelligence on cybersecurity-focused educational topics and some perspective on where we are planning to go in 2024. To that end, we have provided meaningful insights from our expert cybersecurity thought leaders, which we hope you will find both informative and entertaining.

CyberEd's coursework has been vetted and curated by our advisory faculty, which includes many of the most highly regarded CISOs in the industry. Our goal is to provide the highest quality education and training courses anywhere, with easily accessible content that is relevant across every industry segment and modern threat vector. We want to help our subscribers on a path of continual learning while expanding the growth of our collective security consciousness by providing a rich surround of white papers, eBooks, podcasts, blogposts, and opinion pieces so that all learners, regardless of job role or title can find and improve their cybersecurity competency in the easiest and most effective way possible.

CyberEd is reflective upon the key findings and themes circulated this month. The cost of a data breach is still more expensive than ever, and emerging technologies like Internet of Things (IoT), artificial intelligence, cloud security and more are at the forefront of these conversations.

Check out a few of this issue's features:

- Our Inaugural "Get Smarter" Summit, where we explore all of the ways that generative AI will impact cybersecurity and the ways in which we can prepare to deal with a variety of use cases. Joined by partners, Google Cloud, Cisco, Broadcom, Exabeam, Zscaler and Orrick Herrington, we focus on obvious and non-obvious threats about which every CISO and security practitioner needs to be aware.
- We interviewed a member of our CyberEd faculty team, Richard Bird, the Chief Security Officer, Application Programming Interface (API) security, for Traceable.ai, who discusses key challenges in API security.
- A podcast episode featuring former Uber CISO Joe Sullivan as we explore his trial, offering insights and advice for aspiring CISOs and those currently in the role, especially in the context of his guilty verdict.

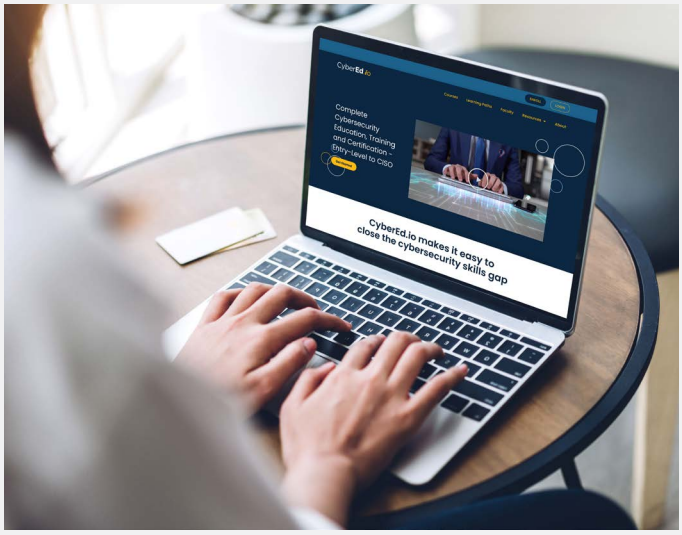
Here's hoping you find worthwhile information in this magazine, and I hope you'll take time to let us know what you'd like to see in the future.

It's your education, and it's our goal to help you achieve your mission.

Best,

Steve King
Senior Vice President, CyberEd.io
Information Security Media Group

NEW COURSES



We're constantly updating the CyberEd.io platform with new course content including lectures from the world's leading cybersecurity and technology experts.

Issues, Topics and Interviews

SPRING	Cover Story: Interview with John Kindervag Learning Path Spotlights: Cloud Security, Risk Analysis
SUMMER	Cover Story: Interview with Chase Cunningham Learning Path Spotlights: Security Warrior, Penetration Testing
FALL	Cover Story: Interview with Richard Bird Learning Path Spotlights: Digital Forensics and ICS
WINTER	Cover Story: Interview with Steve King Learning Path Spotlights: Security Engineering and SOC

CyberEd.io

CyberEd Magazine Editorial

Chief Executive Officer **SANJAY KALRA**
General Manager **MICHAEL D'AGOSTINO**
Senior Vice President **STEVE KING**
Product Manager **KYLE SCHMECHEL**
Executive Editor **BARBARA REIMERS**
Director of Global Creative Strategy **ALEXANDRA PEREZ**
Creative Head **PRASAD ARAWANDEKAR**
Lead Graphic Designer **JINAL CHHEDA**
Social Media Coordinator **PURTIKA PANDEY**

ISMG Editorial

Vice President Editorial **TOM FIELD**
Executive Editor **MARIANNE K. MCGEE**
Executive Editor **MATHEW J. SCHWARTZ**
Managing Editor **GEETHA NANDIKOTKUR**
Managing Editor **TONY MORBIN**
Managing Director **VARUN HARAN**
Director Global News Desk **BRIAN PERIERA**
Editorial Director, News **DAVID PERERA**
Editorial Director **CAL HARRISON**
Principal Correspondent **SUPARNA GOSWAMI**
Director of Production **ANNA DELANEY**

Contact
902 Carnegie Center
Princeton, NJ 08540

Toll Free: (800) 944-0401
ismg.io

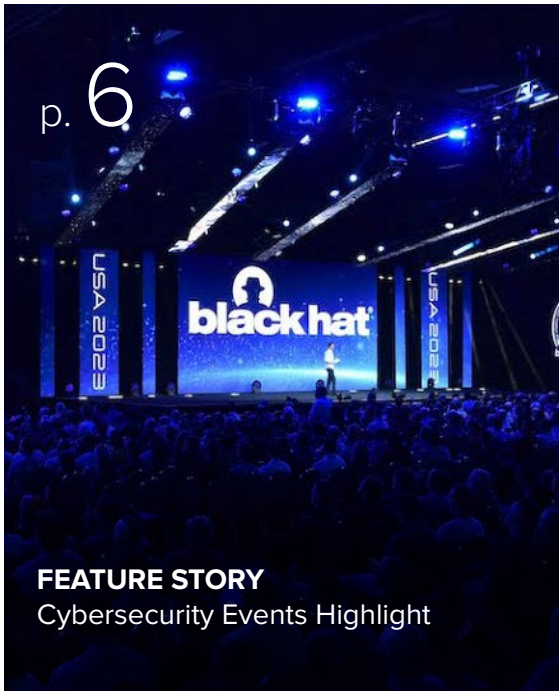
ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Our 35 global media properties provide security professionals and senior decision makers with industry- and geo-specific news, research and educational events.

ismg.io

Table of Contents

INTERVIEW
Overcoming the Inertia of Assessing and Securing APIs p. 10



FEATURE STORY
Cybersecurity Events Highlight

A Roundup of Recent Cybersecurity Events

Takeaways from recent cybersecurity conferences that shine a light on the need for AI integration

In August 2023, Black Hat USA, the world's premier cybersecurity conference, convened, bringing together cybersecurity experts from around the globe to address the latest threats, vulnerabilities, and trends. AI and machine learning dominated discussions, with presentations highlighting their offensive and defensive applications. The cybersecurity skills gap remained a prominent topic, emphasizing the need for more qualified professionals. Expel unveiled its vulnerability prioritization offering, assisting organizations in addressing critical vulnerabilities first.

Dr. Hongyi Wang's presentation, "AI Hacking: How to Hack AI and How to Protect AI Systems," delved into the vulnerabilities and defenses of AI systems. Google's Dr. Eric Grosse presented "The Future of Cybersecurity: A Human-Machine Partnership," emphasizing the importance of collaboration between humans and machines in cybersecurity. Ms. Kiersten Todt's "Closing the Cybersecurity Skills Gap: A Multi-Faceted Approach," addressed the multifaceted approach needed to bridge the cybersecurity skills gap.

The Black Hat Startup Spotlight Competition showcased innovative cybersecurity startups, while the Business Hall featured a wide range of cybersecurity vendors. Networking and social events provided opportunities for attendees to connect with peers and experts. Black Hat USA 2023 proved to be an invaluable event for cybersecurity professionals, offering insights into the latest threats and trends, networking opportunities, and exposure to new cybersecurity solutions.

View this session online at **cybered.io**

BlackHat Vegas 2023

London Cybersecurity Summit

London Cybersecurity Summit

The recent Cybersecurity Summit in London, organized by Information Security Media Group (ISMG), brought together industry leaders to discuss a wide range of crucial cybersecurity topics. AI emerged as a prominent theme during the summit, highlighting its increasing importance in the field of cybersecurity.

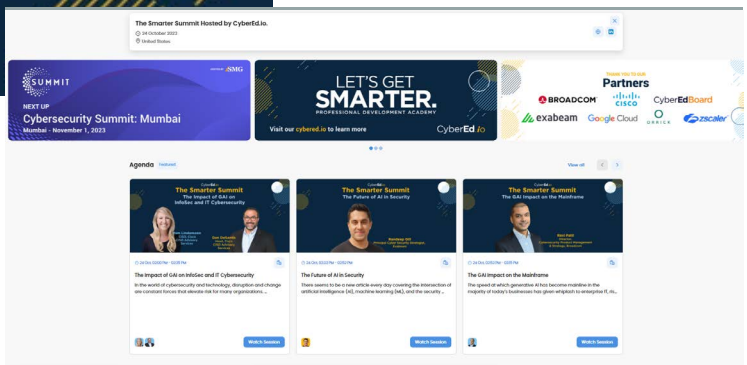
According to Mathew Schwartz, the executive editor of DataBreachToday at ISMG, the security experts on the "Navigating the Technical Landscape of AI" panel delved into the realm of AI beyond the realm of fear, uncertainty, and doubt (FUD). They explored the most promising applications of AI and machine learning, outlined the risks associated with adversarial AI, and shared their experiences regarding the challenges and limitations faced when implementing current AI-driven systems. The panel expressed optimism about the potential security and privacy benefits offered by private generative AI models.

The discussions also revolved around the adoption of AI within organizations, acknowledging the challenges it brings and emphasizing the importance of training security teams to effectively utilize AI. Additionally, there was an in-depth examination of Google's Secure AI Framework (SAIF), which aims to address specific risks associated with AI systems. These risks include model theft, data manipulation, malicious inputs, and the potential extraction of confidential information from training data.

Get Smarter Summit

The most recent Smarter Summit, organized by CyberEd.io, successfully brought together industry thought leaders for a focused exploration of the theme, "The Impact of AI on Information Security." This inaugural summit was conducted in partnership with esteemed companies such as Google, Cisco, Broadcom, Zscaler, Orrick, and Exabeam. The event featured a series of insightful presentations that delved into various facets of AI's influence on information security, including its effects on IT, detection and response strategies, human risk management, uncovering hidden threats, mainframe security, and the evolution of risk discovery.

In addition to its array of distinguished speakers and industry partners, the Get Smarter Summit also featured an AI-generated moderator. This AI moderator played a pivotal role in facilitating discussions and enhancing the overall experience of the event, showcasing the practical applications of artificial intelligence in the realm of information security and conference management.



Richard Bird
Chief Security Officer, Traceable AI

Overcoming the Inertia of Assessing and Securing APIs

A Conversation with Richard Bird

Richard Bird is an internationally recognized identity-centric security expert and Chief Security officer for Traceable AI. He has also been a CIO, CISO, and the global head of identity management for JP Morgan Chase. An internationally recognized data privacy and security expert and speaker, Bird leverages his diverse experiences as a strategic advisor and solutions provider to challenge current notions about cybersecurity. An early proponent of the zero trust strategy, Bird is a frequent speaker on keynote platforms around the world. He is a Forbes Tech Council member and speaks on topics ranging from data protection regulations to cybersecurity-enabled consumer protection.

In a recent interview conducted by CyberEd.io, Richard Bird explores the topic of application programming interface (API) vulnerabilities. He highlights that the majority of organizations, especially those outside highly regulated sectors like banking, have yet to fully comprehend the potential threats associated with APIs.

CYBERED: Is the needle of API security moving positively?

RICHARD BIRD: I think the needle is moving in the right direction. I think there are currently two problems. When I started a year ago, at Traceable AI, I heard many of the same things. I don't have a problem. I've got a web application firewall (WAF), I've got a gateway. I'm going to get around to it. And a year later, I still hear a lot of ideations, a lot of strategy conversations about 'we need to do something, what are we going to do?' I think when we look at tangibly moving the needle, we're seeing that happen in highly regulated industries, specifically banking, -- and there's no banker in tech. It sometimes sounds a little frustrating coming from bankers to say that financial institutions lead the way, but it is the truth. They provide the honeypot of most valuable economic gain for bad actors. Within highly regulated industries, we're seeing heads of API security being stood up, we're seeing API security being talked about, in terms of which part of the organization should it be aligned to from a leadership standpoint, so we are seeing movement in those highly regulated industries. But in most other organizations we're seeing people thinking, pondering and collecting data. At the same time, we're seeing an ever-increasing number of exploits against the API attack surface that would suggest that more people need to be thinking, moving and collecting data -- faster.

CYBERED: How would cybercriminals take advantage of APIs as an attack vector?

RICHARD BIRD: Recently I had a conversation about how hard it is for large enterprise security organizations to shift the direction of their ship. In over 20+ years of this, what I call the cybersecurity 'industrial complex,' cybersecurity organizations have entrenched budgets and entrenched organizational structures and leadership. The comparison

I've made recently, as it relates to bad actors, is that we're trying to fight a war against a guerrilla army that has very small groups or units of people that move quickly. We're trying to fight them with an entire brigade, and everybody knows it's much easier to move a unit than it is to move an entire army. What we're seeing is that there's a huge amount of inertia and friction, to try and orient your organization toward solving API security issues. And yet, the bad actors are moving extremely quickly and discovering even more interesting, new ways to leverage APIs to do bad things.

In fact, there's one important finding that I've had in the last, I'd say, 90 days, that took me aback.

What I saw recently is bad actors are using APIs to conduct combination attacks in the same campaign against a single target, meaning that they're using API volumetric attacks, API application denial of service (DoS) attacks, and then API fraudulent account creation – in other words, three, four, or five different methods. When you think about how security organizations have been structured over the last 20 years, we are almost singularly focused on a plane of attack or a point of attack. So, this idea of bad actors being able to use four, five, six, or seven different types of attacks in one campaign and obfuscating or creating a diversion, while they work to commit the actual crime that they're trying to execute under the covers. That's shocking, and I think that's going to be a big wake-up call for most organizations in the coming year.

CYBERED: Where does this challenge intersect with security teams and their responsibilities because fraud and security teams do not necessarily speak often.

RICHARD BIRD: That is an outstanding observation. Because it's even more complicated than that. I'm fortunate. A number of other companies have been developed over the last couple of years that are specifically in the traditional fraud space — I have friends, colleagues and former bosses who are now running those companies, so I get an opportunity to talk with them. For me, coming out of 17 odd years of banking, I maintain my contacts within the classic fraud organizations. But it's not just that security and fraud teams haven't historically come together. We've seen some movement in that, in the creation of chief security officers and the bringing of fraud teams under CISOs. But that's relatively limited. That's very advanced for most large enterprises. But there are even more complications. Fraud doesn't just touch fraud organizations, it doesn't just touch security organizations, it has implications for legal organizations around data privacy, it has implications for compliance, as we've seen with the Optus or even the Medibank breach in Australia, where the government had to step in and say, 'we're going to have to do loss limits on the laws that we passed on how much you can be fined.' Because the amount of customer data accessed was so massive, Medibank would otherwise be out of business. The mechanics of all the siloed functions within organizations that have never been integrated is that they are now faced with a world in which all of these business functions are knit together with APIs. That lack of coordination or integration is now a 'capitalizable' opportunity for the bad guys. The more that we're all standing around as in the old proverb of 'the six blind men and the elephant,' the more that fraud is going well. Some may say that's not fraud, because it didn't involve a magnetic code swipe. The security people are saying, 'fraud's not our business, that's something for the fraud guys.' The bad guys love this confusion, because it generates a bunch of 'who's on first base' conversations, and we're seeing that type of confusion happening when API breaches and exploits are executed.

CyberEd: What needs to happen now at the identity layer to be able to prevent fraud, and bolster one's security posture?

RICHARD BIRD: I'm a bit of two minds on that question. Because I think there's a certain amount of me that is in the wait-and-see mode. But that wait-and-see mode is also aligned with this big change that I made moving to API security. I'm likely to say identity, the softer side of security, is the gateway for the human element to interact with the digital world. There's a lot of emotion, a lot of tension, and friction that are tied up in how you execute


Richard Bird, Chief Security Officer, Traceable AI

an identity strategy. Historically, though, for all the achievements that we had in the identity space to finally get single sign-on, federation, and authentication in place, we distributed authorization to the wind, to the same application developers that we've distributed APIs to. The reason why I have two minds on what we need to do in the identity space is because I do believe, and I'm saying this cautiously because I am not often considered an optimist. But I'm excited about the possibility of us finally achieving fine-grained access control. When people say, why did you leave identity? I told them no, I didn't leave. I went to API security. That's going to be the sweetspot for identity security in the next two years. More and more security practitioners agree with me on that observation. This idea of putting security guardrails around authorization, where all access, not just to exponential business value, but to discrete access by your mom, your dad, your grandparents, to bank accounts, or specific pieces of information, can be used to help secure their access, post authentication. The implications for a more secure world are big. Here's the thing. We just can't screw it up, like we screwed up all of the preceding things that we've done in security. Like when we spent years sorting out authentication, so that you authenticate once and gain access to everything, meaning that is all I must do to be you and steal your stuff. We can't end up with the same type of poor decisions being made relative to securing in the authorization plane, because we finally have a technological solution that can do it. Let's do it right this time.

CyberEd: What are the other API security gaps you commonly see organizations trying to fill?

RICHARD BIRD: One gap is in functional knowledge about how APIs are exploited. The beautiful thing about APIs; they are coded in such a way that you can divine what it is that they are built for. This allows us to do things like create automated documentation, because, for the last 30 years, application developers notating their code

has been a substantial problem. Being able to use the design specs of the actual read of that API to create documentation, that gives us the information we need to know what it's supposed to do. The reason why that's so important and why there's a knowledge gap on how API exploits work is that bad actors are incredibly clever at making minor adjustments to those APIs over the course of a few days, or weeks, or months, to conduct a 'low and slow' attack. Without a normative baseline capability to compare what an API should be doing to what it is now being used for is what leads directly to the claw hammer analogy, in which the people who designed the claw hammer, designed it for two functions, to drive nails and to pull out nails. Nobody ever expected a hammer to be used for any other purposes until the news broadcasted that somebody used one as a murder weapon. Ok, that is a dark analogy. But the truth is that a hammer designed for one thing can be used to do other things it was never intentionally designed for. And that kind of knowledge gap leads to arguments internally within enterprises about how API security is AppSec. But I can do an app DoS attack. It's on the solutions industry to help enterprises to understand this reality of abuse cases versus use cases, and how they can be encompassed or embodied within the same API. That is a knowledge gap that needs to be closed -- quickly. That may also make improvements on moving that needle that we talked about at the beginning. As people understand this characteristic of APIs, they'll begin to recognize the threat and risks within their organizations.

CyberEd: What are the other API security gaps you commonly see organizations trying to fill?

RICHARD BIRD: I think it's probably a repeat of what I did being a champion for identity, which I haven't stopped doing. I just try and split my work between two Don Quixote causes. But I spend a lot of time now speaking with a much broader and interesting audience. For example, I've recently been asked to be a part of a technology and economic trade mission to several different countries. It's fun to travel. But the reality is it's fun to have conversations with people where maybe some of these security issues are manifesting in different ways within their countries, or their legal structures. There's a lot of that activity going on. For me, it's still keynotes and speaking and being a voice, and ultimately certainly my relationship with ISMG over the years, not simply repeating the company line, but being willing to be diplomatically contentious and try and move the conversation into healthy debate with a recognition that what we've been doing, regardless of the security domain API, or identity, or threat and vulnerability management, that the scoreboard is clearly showing that we're still not yet getting it right. Let's be honest with each other about not getting it right. Let's have an honest dialogue and debate about how to improve API security. That's what I'm staying focused on.

95% of Cybersecurity breaches are caused by human error.

LET'S GET SMARTER.

CyberEd.io is reinventing conventional security awareness with continual learning. Our course library is rich with relevant content for C-suite execs, CISOs, senior practitioners, entry-level employees, and staff typically not involved with cybersecurity in their daily job duties. We build Cyber-Warriors at every level.

CyberEd.io

375.456.3350 | Cybered.io | info@cybered.io

Unlocking the Cybersecurity Hiring Gap

Highlights from CyberEd's New Survey Report

A lack of qualified candidates underscores the need to close the cybersecurity skills gap. This shortage of qualified candidates is only exacerbated by an ongoing absence of diversity in cybersecurity roles. In total, more than half of respondents (55%) from our recent online survey cited an inadequate or poor availability of qualified candidates. Approximately two thirds of respondents (67%) cited an inadequate or poor availability of qualified female candidates.

The availability of early career candidates was found to be adequate or better by 56% of respondents. This appears to coincide with recent growth in cybersecurity educational programs and providers, enabling more students to choose a cybersecurity career path, although it appears that the growing availability of training is still not enough to close the gap in filling early-career job roles.

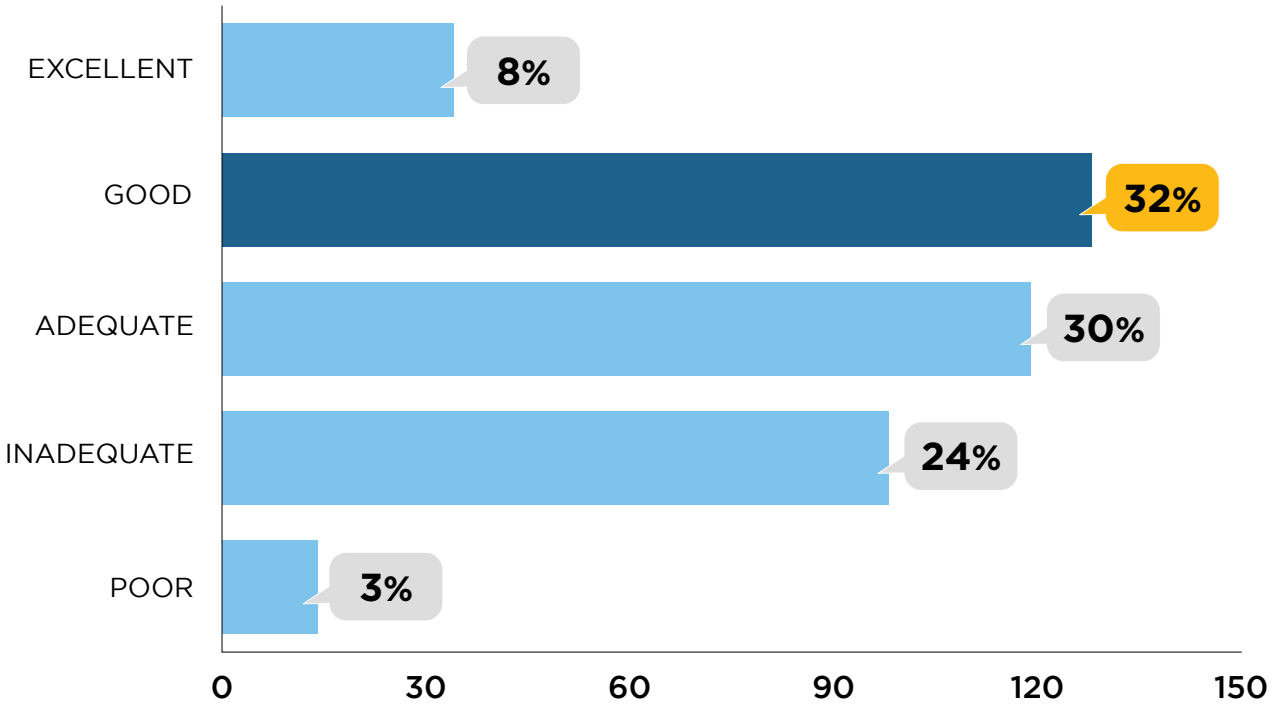
Here are a few additional findings from our recent CyberEd online survey, available here.

Cybersecurity Competency

Most departments are perceived as 'cybersecurity competent,' with IT cited most often as having the highest competency. In addition to this, approximately 70% of respondents described their company-wide cybersecurity training as adequate or better. If this is the case, why are companies still suffering from increasingly worse cyberattacks?

Unfortunately, responses regarding tilting toward 'adequate or better organization-wide cybersecurity training' demonstrate a clear disconnect between what's perceived as effective – and what's adequate. Many cybersecurity breaches originate through phishing or associated social engineering attacks – 90% or more, according to industry estimates. Yet organizations typically perform awareness training activities once per quarter, or less often. The survey indicated that only slightly more than a third of respondents (36%) said their organizations provide enterprise-wide cybersecurity awareness training. All of this falls short, failing to close 'inadequate cybersecurity awareness' gaps.

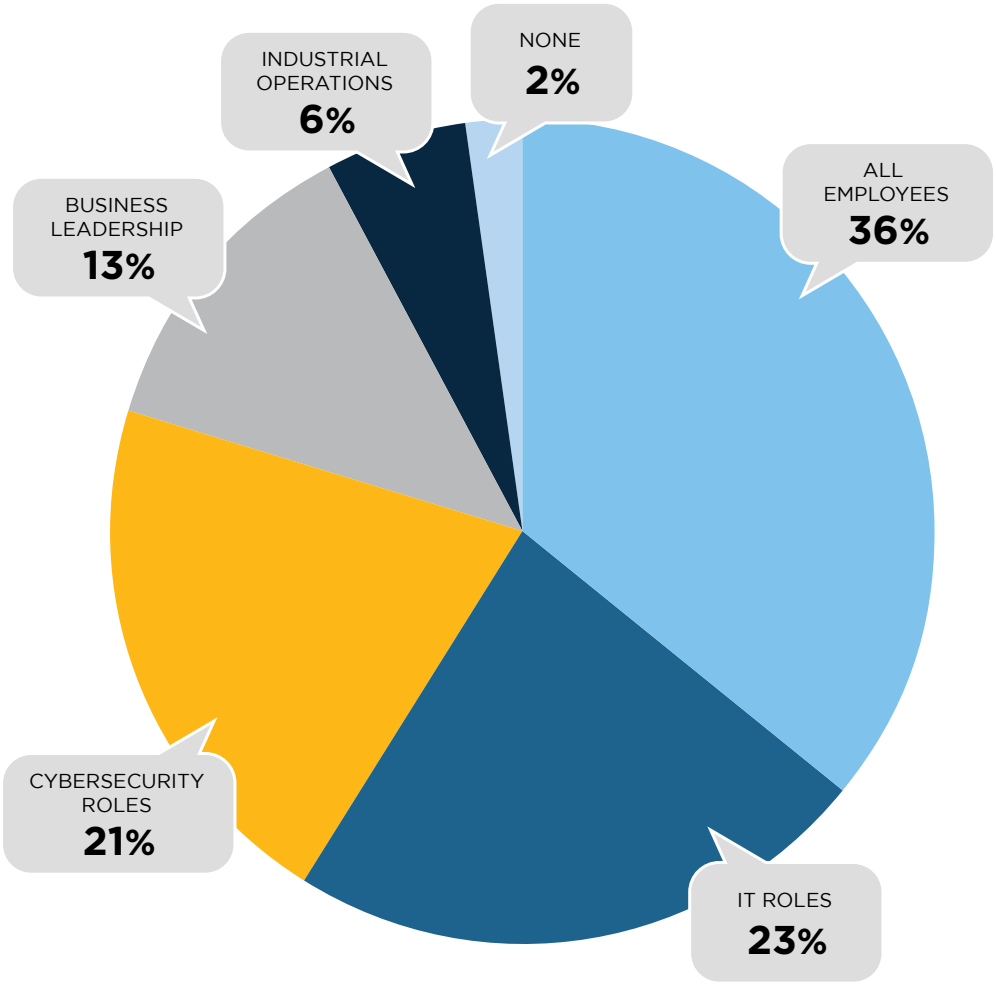
AVAILABILITY OF EARLY CAREER CANDIDATES



Availability of Cyber Training

Slightly over 1/3 of respondents (36%) said cybersecurity training is offered for all employees. That leaves nearly 2/3 of organizations without comprehensive cybersecurity training and education.

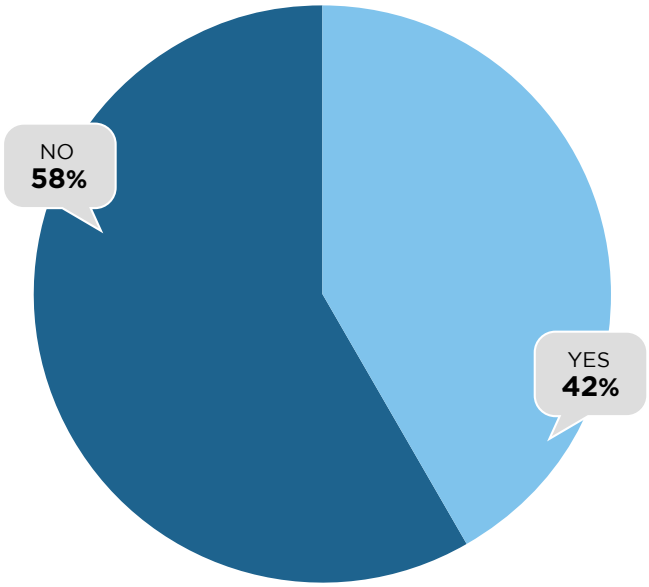
A total of 44% of respondents reported that training was offered for IT and cybersecurity roles, which is relatively low given the strong demand, and in light of requirements for ongoing education across all levels of IT and cybersecurity jobs.



Time to reconsider?

Given rising cyberthreats, it's a wise move to equip cybersecurity professionals with the latest training and certifications to keep their skills sharp. Training and reskilling programs are beneficial for employees and organizations alike, providing a positive impact on employee retention. At the same time, all types of organizations benefit from well-trained, up-to-date cybersecurity teams. By investing in training programs and certifications, organizations can even help to foster non-cybersecurity personnel to consider moving into the cybersecurity field for career advancement opportunities. Employees are generally less tempted to seek new jobs if they believe their current employers are invested in their skill development and willing to provide opportunities for growth.

Approximately 58% of respondents currently offer no cybersecurity training tuition reimbursement. This is something to reconsider as organizations work to mitigate risks and improve cybersecurity protections.



Training matters

Rising numbers of cyberattacks underscore the need for greater training across all departments and job roles. Since the onset of the global pandemic, for example, the FBI has reported up to an 800% increase in cyberattacks. This is why it's important to increase your organization's focus on training for all employees. Consider investing in a continuous managed service training approach, to keep your personnel informed, educated and updated on how to spot scams, and what to do to avoid such attacks.

Learn more about CyberEd's online research study and what we learned here.

The global average cost of a data breach in 2023 was U.S. $4.45 million, a 15% increase over 3 years.

LET'S GET SMARTER.

CyberEd.io is reinventing conventional security awareness with continual learning. Our course library is rich with relevant content for C-suite execs, CISOs, senior practitioners, entry-level employees, and staff typically not involved with cybersecurity in their daily job duties. We build Cyber-Warriors at every level.

CyberEd.io

375.456.3350 | Cybered.io | info@cybered.io

CyberEd Featured Faculty

RICHARD BIRD

Chief Security Officer, Traceable AI

Richard Bird is an internationally recognized identity-centric security expert who has been a CIO, CISO, and the global head of identity management for JP Morgan Chase. An internationally recognized data privacy and identity-centric security expert and global speaker, Bird leverages his diverse experiences as a strategic advisor and solutions provider to challenge current notions about cybersecurity. An early proponent of the zero-trust strategy, Bird is a frequent speaker on keynote platforms around the world. He is a Forbes Tech Council member and speaks on topics ranging from data protection regulations to cybersecurity-enabled consumer protection.

DR. CHASE CUNNINGHAM

VP, Security Market Research, G2

Dr. Chase Cunningham, known as the Doctor of Zero Trust, Dr. Cunningham is an early advocate and proponent of the Zero Trust strategy and is currently the VP of Security Market Research for G2. In this role, Dr. Cunningham shapes the company's strategic vision, roadmap and key partnerships. Dr. Cunningham previously served as vice president and principal analyst at Forrester Research, providing strategic guidance on Zero Trust, artificial intelligence, machine learning and security architecture design for security leaders around the globe.

SAM CURRY

VP, CISO, Zscaler

Sam Curry is a 30-year veteran employee at Signal 9 Solutions, a start-up that invented the personal firewall, executed the first commercial implementation of Blowfish, and devised early stealthy (symmetric key) VPN technology that was ultimately sold to McAfee. Curry would go on to serve as Chief Security Architect there and as head of Product for McAfee.com before holding several positions at RSA including head of RSA labs at MIT, head of product, and CTO, as well as Distinguished Engineer for EMC. After seven years with RSA, Curry acted as SVP and CISO at Microstrategy, CSO & CTO for Arbor Networks before it became Netscout, and as CSO for Cybereason.

KELLY HOOD

EVP and Cybersecurity Engineer, Optic Cyber Solutions

Kelly Hood is an EVP and cybersecurity engineering expert supporting organizations across sectors to develop and implement strategies to manage cybersecurity and privacy risks to their business. She works with organizations to meet cybersecurity best practices, controls and standards, including the NIST Cybersecurity Framework, CMMC, SP 800-53, SP 800-171 and ISO 27001. She assisted the NIST Cybersecurity Framework team in the evolution and outreach of the Cybersecurity Framework.

CLIFF KITTLE

Technical Cybersecurity Content Developer/Writer, Strategist

Cliff Kittle is responsible for increasing the awareness of Dell SecureWorks' ability to assist healthcare providers and business associates in their efforts to strengthen their security posture. Kittle speaks regularly on the importance of an Information Security Program and its elements.With more than 36 years of experience in technology solutions and 10+ in information security, Kittle has worked in fields such as biometric authentication, identity access management and single sign-on, privileged user access control, and information security management systems based on ISO 27001.

TAL KOLLENDER

CEO, GYTPOL

Tal Kollender is the CEO and co-founder of GYTPOL, a privately held security compliance company that focuses on policy validation and detection of configuration weaknesses. Kollender, A self-taught teenage hacker, she had her sights set on flying fighter jets in the IDF, but though she qualified, she was whisked off to Cybersecurity duty in the Cyber Security-Systems Division, where she served as an ICT cyber specialist. Her professional career took her to Dell EMC where she was cyber expert and System Security Architect before creating Gytpol with her co-founders. In 2023, Tal received the Entrepreneur of the Year award from the United Cybersecurity Alliance.

JIMMY MESTA

Co-Founder & Chief Technology Officer, KSOC

Jimmy Mesta is the Co-Founder and Chief Technology Officer at KSOC, the organization that triages risk across Kubernetes clusters in real time. He is responsible for the technological vision for the KSOC platform. Mesta, veteran security engineering leader focused on building cloud-native security solutions, Jimmy has held various leadership positions with enterprises navigating the growth of cloud services and containerization. At the Web App Firewall Innovator Signal Sciences (acquired by Fastly, Inc.), he led offensive and defensive teams across the Security and Engineering organizations while helping build modern, developer-friendly security solutions.

LYNN PEACHEY

Director of Business Development, Arete Incident Response

Lynn Peachey is an expert in the cyber insurance space. Currently, she serves as the director of business development, connecting clients and partners with cybersecurity solutions at Arete Incident Response, an insurance company and security insurance space. Previously earning her two bachelor's degrees from Rutgers University in New Jersey in psychology and industrial relations, then her JD from Pace University's Elizabeth Haub School of Law, Peachey is licensed in multiple states, including New York, California, Texas and Florida, as well as admitted to the New York and New Jersey Bar.

Memo to CISOs

About Living an Asymmetric Life

STEVE KING
Senior Vice President,
CyberEd.io

Graham Weaver is the CEO of Alpine Investors, a San Francisco investment firm that reported $9.7 billion in 2022 revenue. He spoke to the 2023 graduating class of Stanford's Graduate School of Business on “How to Live an Asymmetric Life.”

Here’s what he said.

Louis Pasteur discovered two kinds of molecules in nature: those that, like water, occur only in one spatial conformation and those that, like tartaric acid, can occur in two, such that one is the mirror image of the other. The technical term is “chirality,” from the Greek kheir (hand). Our hands are an excellent example of chiral asymmetry. Just put one on top of the other. They do not match, which is why you don't want to have two left-handed gloves.

He discovered that the universe was asymmetric, that while amino acids, and the ingredients that chain up to make proteins, are “left-handed,” sugar molecules are “right-handed.” No one knows why, but the amazing existence and persistence of asymmetry define the basic components of all living systems.

Here is my version of Weaver's 4 principles for an asymmetric life:

Principle 1

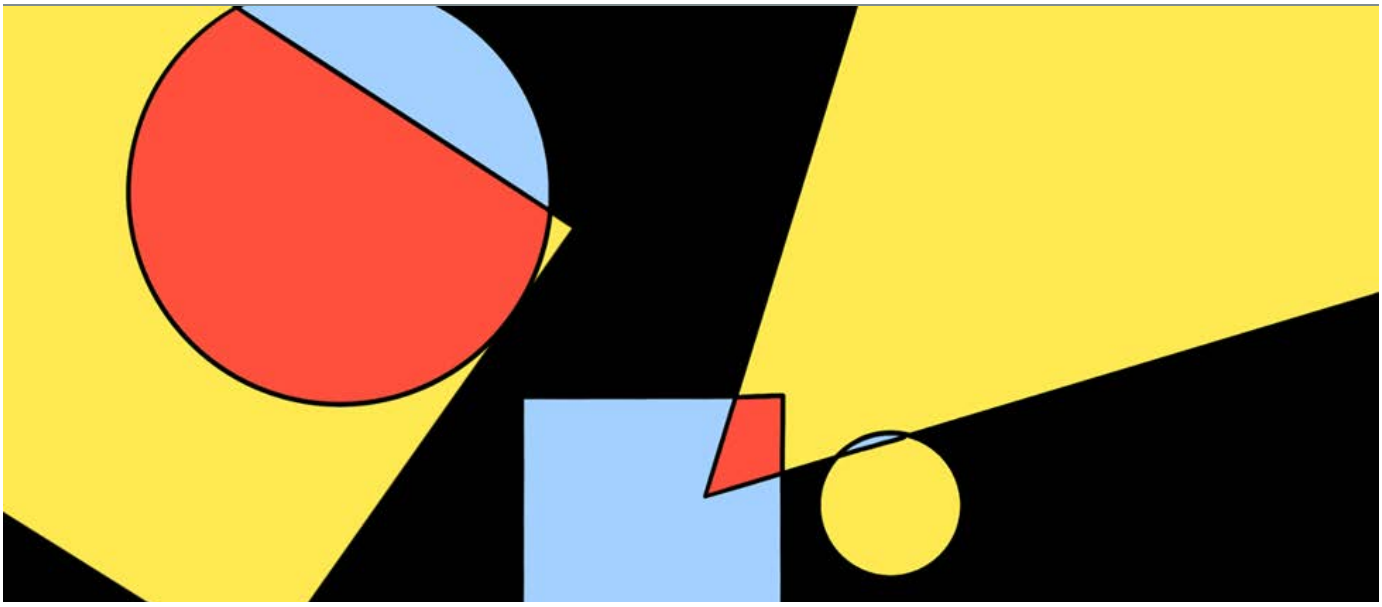
Do hard things

Any change that you want to make is always going to be hard at first. The biggest driver of that curve is fear. Accept this and go do hard things anyway.

Principle 2

Do YOUR thing

Buddha told us 2800 years ago that no matter what path we choose, we will have suffering. Life is suffering. So, choose something worth suffering for. And do it.



Principle 3

Do it for a long time

You can be the best there is, but it will not happen overnight. You need to keep doing it. Until you get it right. Until you are the best. And, then you'll need to do it more. Vince Lombardi once said the Green Bay Packers never lost a football game, but every now and then, they ran out of clock.

Principle 4

Don't write a story about what happens

Don't write a story about what happens; write your story and then make it happen. You will never win trying to execute someone else's dream.

These 4 principles are the antidote to fear.

I know that every one of us is capable of turning back the tide of adversarial cyberattacks - if we don't know exactly what to do, we can learn what to do.

We are surrounded by smart people, all of whom are happy to share their knowledge and advice. We know we need decision-makers on our side. We also know we are the ones to convince them to do what it takes. Being a CISO is not easy. We need to break through doubt and uncertainty in a complex domain.

We can start by doing the hard things.

Cybersecurity Insights Podcast

The Joe Sullivan Case

Joe Sullivan is a lawyer and a CISO, and a former federal prosecutor with the United States Department of Justice. He served as a CSO at Facebook, Uber, and Cloudflare and as an associate general counsel at PayPal.

Sullivan co-founded the Computer Hacking and Intellectual Property unit at the Department of Justice, DOJ, and worked there for 8 years. He served as a commissioner at the National Cyber Security Alliance for 5 years and became a board member of the National Action Alliance for Suicide Prevention and co-authored the "2012 National Strategy for Suicide Prevention." Additionally, he was appointed as commissioner of the Commission on Enhancing National Cybersecurity by President Obama in 2016.

In August 2020, the DOJ charged him for obstruction of justice in the 2016 Uber data breaches. The criminal complaint said he arranged, with CEO Travis Kalanick's knowledge, to pay a ransom disguised as a "bug bounty," and falsified non-disclosure agreements with the hackers to say they had not obtained any data. In December 2021, he faced additional charges of wire fraud.

In 2022, Sullivan was convicted of one count of obstruction of justice and one count of misprision of felony and sentenced to three years of probation and a million hours of community service. This prosecution represented the first United States federal prosecution of a CISO for the handling of a data breach.

In 2023, he took on the role of CEO of Ukraine Friends, a nonprofit focused on humanitarian aid to Ukraine.

In this episode of Cybersecurity Insights, Joe discusses:

- His perspective on what transpired;
- How this verdict impacted his life;
- Insights and advice for future CISOs and those currently holding the role in light of the verdict;
- And much more.

Learn more by listening to the podcast here.

Cybersecurity Insights Podcast

The Dangers of Generative AI in Incident Response

Alex Waintraub is a DFIR Expert Evangelist at CYGNVS, a first-of-its-kind, guided cyber crisis preparation and response platform. He has more than a decade of experience leading SOCs, incident response plans, threat intelligence operations and cyber threat hunting teams' response, containment, and remediation methods. Prior to joining Cygnus, Alex served as VP of Incident Response for BNY Mellon, as well as led incident response and cyber operations at Barclays Investment Bank and BlueVoyant.

In this episode of Cybersecurity Insights, Alex discusses:

- ChatGPT's role in Incident response;
- What Cygnus does and its business model;
- How AI helps in cybersecurity defense;
- And much more.

Learn more by listening to the podcast here.

Cybersecurity Insights Podcast

Exploring AI and Network Security

Pam Lindemoen is a CISO Advisor in Cisco's Security Organization. She is an Information Security executive leader with over 25 years of experience within the IT industry. Pam joined Cisco from Anthem, Inc. where she held the Deputy Chief Information Security Officer role. While at Anthem, she was considered a bold and strategic thinker who envisioned and delivered a world-class Enterprise Information Security strategy, including the Steering Committee with cross-functional business and technology membership.

Dan DeSantis is the Director, CISO Advisory in Cisco's Security Organization. He has 25 years of experience as a tech founder, Chief Technology Officer, and as a leader working with many of the largest companies in the world. He rejoined Cisco in 2020 from Focal Point Data Risk where he co-led efforts across advisory, identity and cyber workforce development practices.

In this episode of Cybersecurity Insights, Dan and Pam discuss:

- Generative AI vs Discriminative AI in Cybersecurity defense;
- Comparing the upside of G-AI opportunities to the downside of new threats;
- The future of network security;
- And much more.

Learn more by listening to the podcast here.

Cybersecurity Insights Podcast

Real-Time Financial Fraud

Alisdair Faulkner is co-founder and CEO of security and fraud prevention startup Darwinium, and co-founder and former CPO of ThreatMetrix (later acquired by LexisNexis Risk Solutions for $830M). Alisdair is based in Sydney, Australia, and has more than two decades of experience in the cybersecurity space with a career-long passion for analyzing and preventing financial fraud. Darwinium services large B2C organizations and marketplaces, dedicated payments providers, ecommerce shops, banks, and some fintechs.

In this episode of Cybersecurity Insights, Alisdair discusses:

- How have popular cash transfer apps like Zelle, Venmo, Cashapp, and PayPal become avenues for fraudsters to scam users out of thousands?
- Does the launch of the U.S. Federal Reserve's real-time payment tool, FedNow, raise concerns about potential security risks due to the widely unregulated nature of the space?
- What measures and safeguards can be implemented to prevent the occurrence of fraudulent activities and misappropriation of funds?
- And much more.

Learn more by listening to the podcast here.

CyberEd ICS/OT SECURITY WARRIOR

- ICS/SCADA Security Fundamentals
- Network Traffic Analysis for Incident Response
- Identity and Access Management
- SCADA Security Architecture
- SCADA Cyber Range
- Cyber Threat Hunting
- Cyber Threat Hunting Cyber Range

CyberEd SOC WARRIOR

- Incident Response Tactics
- Network Traffic Analysis
- Network Traffic Analysis Cyber Range
- Cyber Threat Hunting
- Cyber Threat Hunting Cyber Range
- Advanced Intrusion Detection

Learning Path Spotlights

CyberEd.io is a new category of online education in cybersecurity, designed to provide all of the fundamental baseline technical skills necessary to train Cyber-Warriors in the art of detection, defense, and protection, while also instilling in our members the perspective on why reasoning matters, why adaptability matters, why thinking like hackers matters, and how they can contribute to growing a culture of cybersecurity and increase their culture of cybersecurity and an appetite for continuous learning.

When we partner with a customer, we partner for life. Our mission is to help defeat our adversaries on all fronts.

Our platform provides a rich context within which students have access to white papers and eBooks written by industry experts, and with case studies that bring the training to life. Our podcasts dive deep into new technologies and processes that are working against our adversaries. Our daily blog posts always keep us on the mission path and focused on our objectives and key outcomes.

Our Master Class series is taught by widely recognized cybersecurity thought leaders and can only be found on CyberEd.io.

We have hundreds of summit sessions from around the world to help our students understand what matters and why, in Singapore, Italy, India, Hong Kong and elsewhere around the world.

All of our content is refreshed weekly and much of it is presented by a friendly team of avatars who do a remarkable job of instructional delivery.

Our industry needs more experts and analysts to execute and examine cybersecurity solution frameworks, more DevSecOps experts to reinforce continuous integration and continuous delivery (CI/CD) pipeline security, along with more and better trained security engineers, researchers, and leaders than our enemies can train.

We will continue building better teams, driving better results, creating greater unity and engineering a cybersecurity culture within every customer organization with which we partner.

In this issue, we highlight two Cyber-Warrior learning paths:

- ICS/OT Security Warrior
- SOC Warrior

ICS/OT SECURITY WARRIOR

Secure the critical industrial systems in your organization and improve your factory supply chain security with the CyberEd Industrial Control Systems/Operational Technology (ICS/OT) Warrior pathway. Attacks on industrial control infrastructure are occurring with increasing frequency and strength. Control systems across the globe need strong Infosec teams behind them to ensure these threats do not succeed. CyberEd's industrial control system certifications cover what ICS professionals need to know: how to protect and defend critical industrial systems and respond to incidents that will inevitably occur across the entire OT infrastructure.

SOC WARRIOR

In the CyberEd.io Warrior Training, there are three levels of achievement, all of which we teach to ensure that security teams are adequately prepared to fight their adversaries on the front lines. The Tier 1 SOC analysts serve as the first line of defense in cybersecurity operations, diligently monitoring security systems, managing and fine-tuning security tools, assessing the criticality of incidents, and escalating them as required. Tier 3 SOC analysts operate as cyber threat hunters, proactively scouring the network for vulnerabilities and elusive cyber threats.

LET'S GET SMARTER.

Talk to an CyberEd Expert Today

CyberEd.io

CyberedIo

CyberEd.io

CyberEd.io

Visit cybered.io