SPRING 2024

CyberEd MAGAZINE

COVER STORY INTERVIEW

AI and the Art of Cyber Defense

Insights from Sam and Red Curry

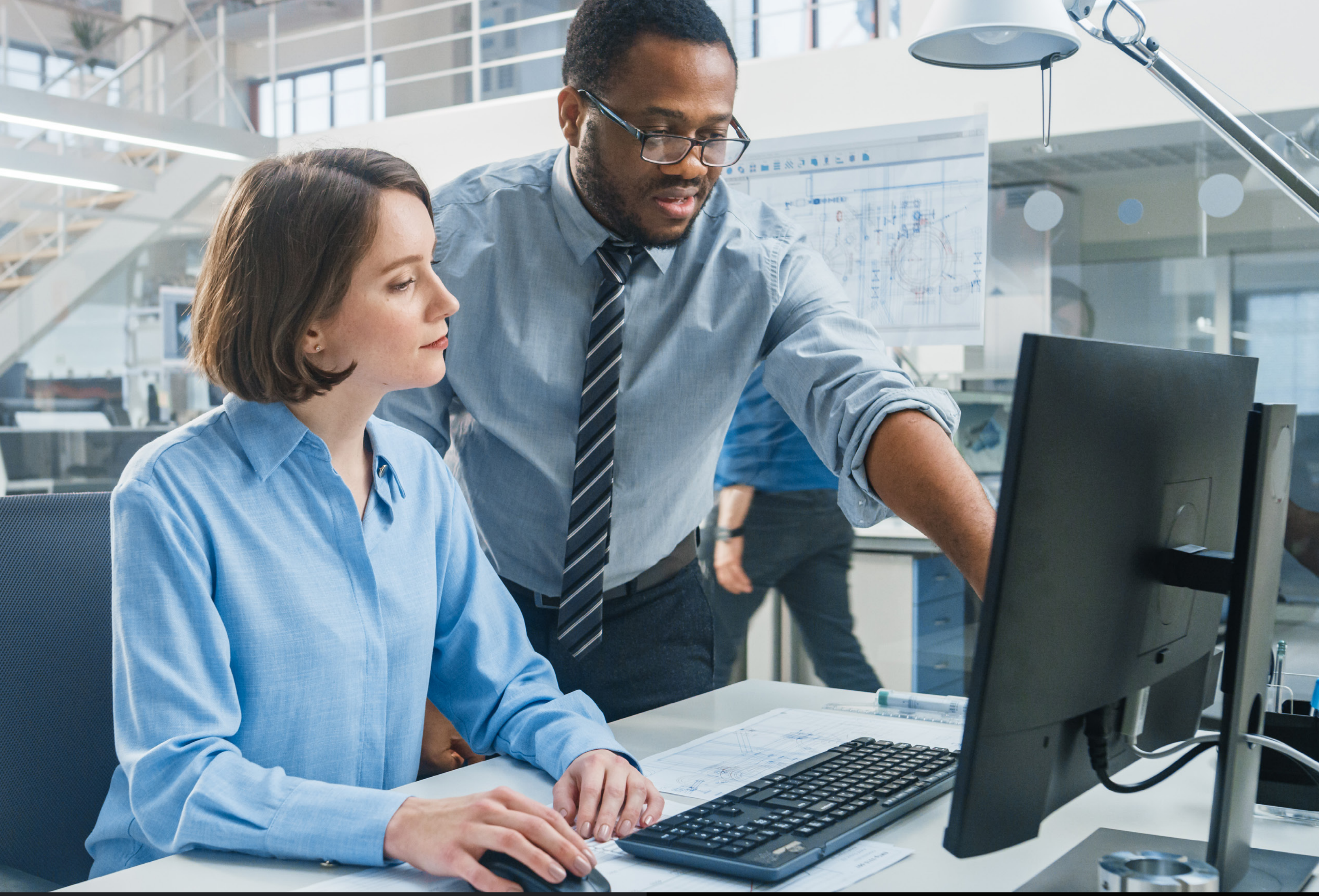
PAGE 14

AI Uncertainties: Enhancing or Eroding Education?

PAGE 6

Red Curry
Chief Marketing Officer,
vFortified LLC

Sam Curry
Global VP, CISO,
Zscaler



Letter from the Senior Vice President

Welcome to the Spring 2024 edition of CyberEd Magazine! We're excited to have launched our revolutionary advancement in Security Awareness Training – our new Human Risk Management (HRM) platform.

This breakthrough platform marks a significant leap forward, as it fully leverages a catalog of security apps and appliances that you, the customer, may likely have already installed in your own shop. From tracking employee behavior in your computing environment, you identify in real-time the employees who need specific training in operational protocols such as passwords, multifactor authentication (MFA), identity and access management (IAM), phishing, and others.

As a result, we apply this training from our extensive catalog and monitor the results. Over time, our customers see a clear reduction in human risk scores, removing vulnerabilities from attack surfaces before they occur.

LivingSecurity is not just our exclusive HRM partner. They have continuously made Gartner's and Forrester's lists of top 3 products in Gartner's Magic Quadrants and Forrester's Wave rankings, with top GTM strategies. Many traditional market leaders in security awareness training haven't developed these capabilities.

Based on a digital ecosystem that's more than reactive, but prescient, tailoring its risk factoring to the unique behavioral patterns of each individual user, the training offered is targeted, and highly personal – designed to address the specific behaviors that drive a high risk score. This is a far cry from the blanket security training approaches of yore.

The apps detect and flag aberrant behaviors attempting to work around MFA policy, permission controls and configuration protocols. They include all of the key indicators for phishing/email attacks, endpoint strikes, malware, data loss, account compromise, credential hygiene and MFA. These indicators are mapped to AD to quickly identify in real-time who is doing what, where, to help organizations address each issue as soon as a risk score exceeds a pre-determined threshold.

This SmartHRM™ is changing how we detect insider threats and making us all safer.

Also in this issue, check out our Events Roundup, along with an engaging, sometimes intense, and always entertaining interview with the Curry Brothers, an insightful glimpse into a recent IDTR research report, a blog about the positive and negative impacts of AI on education, and a quick review of new learning paths.

We're excited to lead this new era in cybersecurity consciousness and look forward to sharing all of these insights and resources with you.

Warm regards,

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

Steve King

Senior Vice President,
CyberEd.io

Steve is a seasoned technology executive with more than 25 years of experience in the cybersecurity industry. He is currently Senior Vice President for CyberEd.io, the cybersecurity education division of ISMG. He began his career as the West Coast managing partner of MarchFIRST, Inc. overseeing significant client projects, and later founded Endymion Systems, which was eventually acquired by IBM. Throughout his career, Steve has held leadership positions in startups, such as VIP/SeeCommerce and Netswitch Technology Management, contributing to their growth and success.

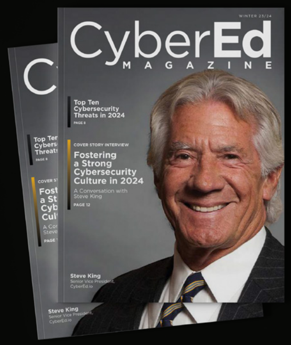
CyberEd.io
Introducing the CyberEd.io SmartHRM™ Solution
A Completely New Approach to Cybersecurity Education, Training and Certification, from Entry-Level to CISO
The End of Traditional Security Awareness Training!

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.

Previous Issues

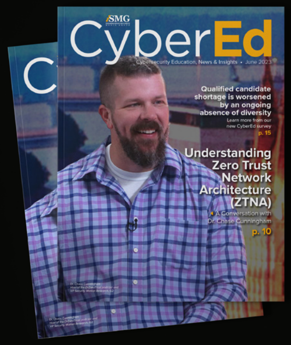
See our prior CyberEd Magazine issues below:


CyberEd MAGAZINE
Top Ten Cybersecurity Threats in 2024
Fostering a Strong Cybersecurity Culture in 2024
A Conversation with Steve King
Steve King

Winter 23/24

CyberEd.io
Perceptions versus reality:
p. 16
Overcoming the Inertia of Assessing and Securing APIs
A conversation with Richard Bird
p. 10
ISMG

Fall 2023


CyberEd
Qualified candidate shortage is worsened by an ongoing absence of diversity
p. 15
Understanding Zero Trust Network Architecture (ZTNA)
A conversation with Dr. Chase Cunningham
p. 10

Summer 2023

CyberEd
Welcome to our inaugural issue!
p. 6
Mitigate Risks with Zero Trust
A conversation with John Kindervag
p. 8

Spring 2023

CyberEd MAGAZINE

CyberEd Magazine Editorial
Chief Executive Officer **SANJAY KALRA**
General Manager **MICHAEL D'AGOSTINO**
Senior Vice President **STEVE KING**
Dir. of Content Dev. and Managed Services **KYLE SCHMECHEL**
Executive Editor **BARBARA REIMERS**
Director of Global Creative Strategy **ALEXANDRA PEREZ**
Lead Graphic Designer **CAITLIN PERSICHILLI**
Social Media Coordinator **PURTIKA PANDEY**

ISMG Editorial
Senior 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 34 global media properties provide security professionals and senior decision makers with industry- and geo-specific news, research and educational events.

www.ismg.io

Table of Contents

COVER STORY INTERVIEW

AI and the Art of Cyber Defense

Insights from Sam
and Red Curry

PAGE 14

Learning Path Spotlights

PAGE 34

AI Uncertainties: Enhancing or Eroding Education?

By Steve King

While the advent of Generative Pre-trained Transformer (GPT) technologies has ushered in a new era of possibilities in education, from facilitating personalized learning experiences to offering unprecedented access to information, the new era brings along some drawbacks as well.

The potential negative impacts on education, particularly in the areas of dependency and academic integrity, merit a closer examination to fully understand their implications and to develop strategies for mitigation.

DEPENDENCY: REDUCED CRITICAL THINKING

One of the most pressing concerns with the proliferation of GPT in educational settings is the risk of reduced critical thinking among students.

We stopped teaching Critical Thinking over 30 years ago in public schools and many would argue it has yielded the society and culture we have today.

Critical thinking – the ability to analyze facts, generate and organize ideas, defend opinions, make comparisons, draw inferences, evaluate arguments, and solve problems – is a foundational skill in all areas of education. While almost non-existent now in public education, the impact of AI will be to eliminate what little is left.

It's the old HP Calculator analogy – why do I need to know how math works if I can just solve equations with a device?

When students turn to GPT for quick answers, there is a significant risk that they decide to bypass the cognitive processes involved in critical thinking altogether.

This is known as leaky abstraction. The convenience of obtaining immediate answers discourages students from engaging in the mental rigor required to explore topics, analyze different perspectives, and develop their own reasoned arguments. This shift will stifle intellectual curiosity and diminish the development of critical thinking skills that are crucial for informed citizenship. Over time, they will erode any fundamental knowledge of the domain under study and soon we will only know that a domain is necessary, but not why.

DIMINISHED LEARNING EFFORT

Moreover, the ease of generating essays and assignments using GPT will lead to diminished learning effort. When students rely on AI to complete their work, they miss out on the learning experiences that come from engaging deeply with content, conducting research, and synthesizing information.

This reliance on technology can create a passive learning environment where students are consumers rather than active participants in their education. Over time, this results in a superficial understanding of subjects, with students lacking a deep or nuanced grasp of the material. The convenience offered by GPT, while appealing, will ultimately detract from the rigorous learning process that is essential for academic and personal growth.

ACADEMIC INTEGRITY: PLAGIARISM AND CHEATING

The issue of academic integrity is another significant concern in the context of GPT's influence on education. As GPT technologies make it increasingly easy to generate sophisticated essays and complete assignments, the temptation for students to pass off AI-generated work as their own grows.

This not only raises questions about the authenticity of students' work but also undermines the principles of academic integrity that are fundamental to the educational process.

Plagiarism and cheating, facilitated by GPT, compromise the fairness and credibility of academic assessments, devaluing the educational achievements of all students.

Addressing this challenge requires a reevaluation of how assignments are designed and assessed, with a greater emphasis on tasks that encourage original thought and creativity that cannot be easily replicated by AI.

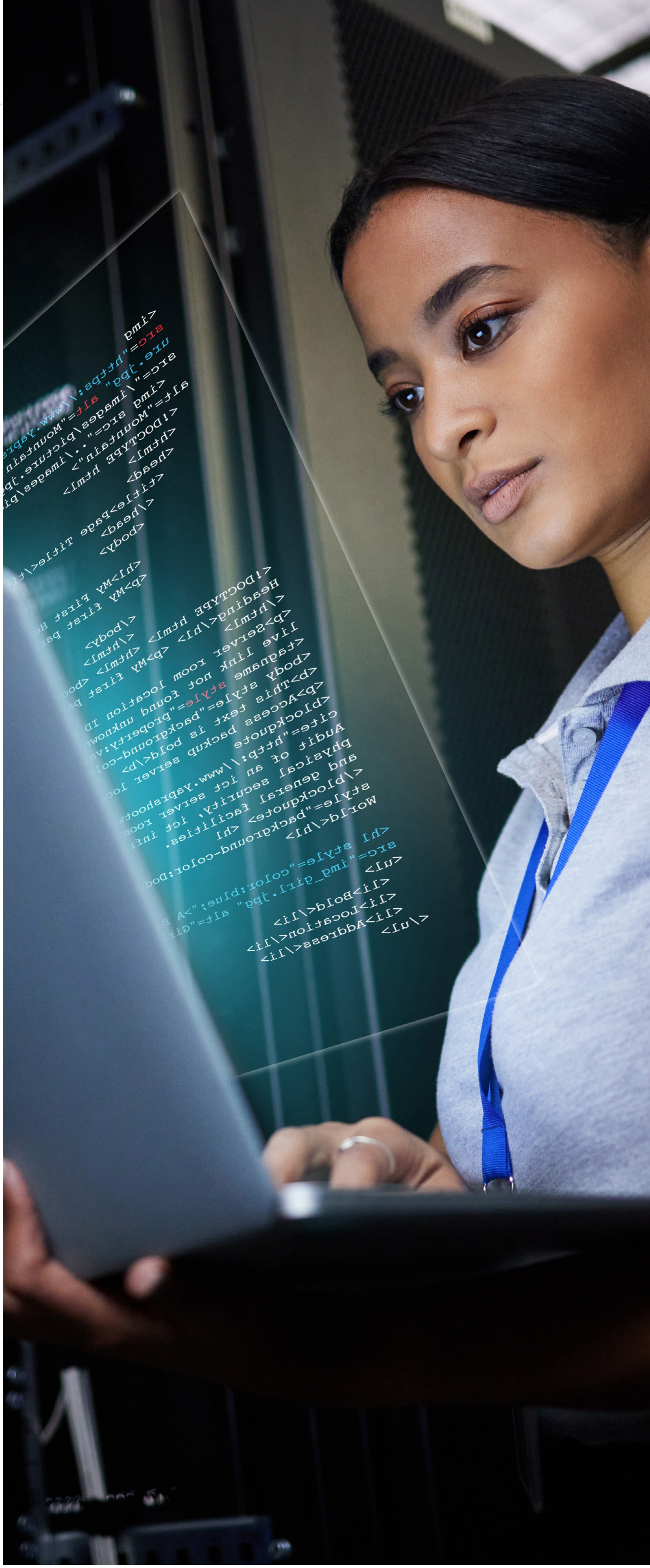
EROSION OF WRITING AND SPEAKING SKILLS

Finally, the dependence on GPT for writing assignments also poses a threat to the development of students' writing skills. Writing is a complex process that involves more than just stringing words together; it requires the ability to articulate thoughts, structure arguments, and convey ideas clearly and persuasively. When students rely on AI for these tasks, they miss out on the opportunity to practice and refine these skills.

Over time, this will lead to an erosion of writing and speaking abilities, with students becoming less capable of expressing themselves effectively without the aid of technology. The impact of this on students' future academic and professional prospects cannot be overstated, as strong writing and speaking skills are a prerequisite for success in almost every field.

THE GENIE IS OUT. THERE'S NO GOING BACK.

The integration of GPT into educational practices presents a paradox. On one hand, it offers tools that can enhance learning experiences in unprecedented ways. On the other hand, it poses significant challenges to the foundational



aspects of education: critical thinking, learning effort, academic integrity, and the development of essential skills.

Addressing these challenges requires a multifaceted approach. Educators must be proactive in designing curricula that leverage the benefits of GPT, while mitigating its negative impacts. This might include developing new assessment strategies that prioritize originality and critical engagement with material, as well as incorporating activities that emphasize the development of critical thinking and writing skills.

Furthermore, there is a need for ongoing dialogue among educators, policymakers, and technologists to navigate the ethical considerations surrounding the use of GPT in education.

Only through collaborative effort can we ensure that the integration of AI into educational settings enriches the learning experience without compromising the core values and objectives of education.

The goal should be to harness the power of GPT as a tool for enhancing education, rather than allowing it to undermine the very foundation of the educational process.

CyberEd Spring 2024 Events Roundup

UNLOCKING THE FUTURE AT THE "GET SMARTER SUMMIT"

Join ISMG and CyberEd for the upcoming "Get Smarter Summit" on April 24th. Proudly sponsored by industry leaders Broadcom, LivingSecurity, CMU, and Unstoppable Domains, this summit marks the shift toward safeguarding our digital landscape through Human Risk Management (HRM).

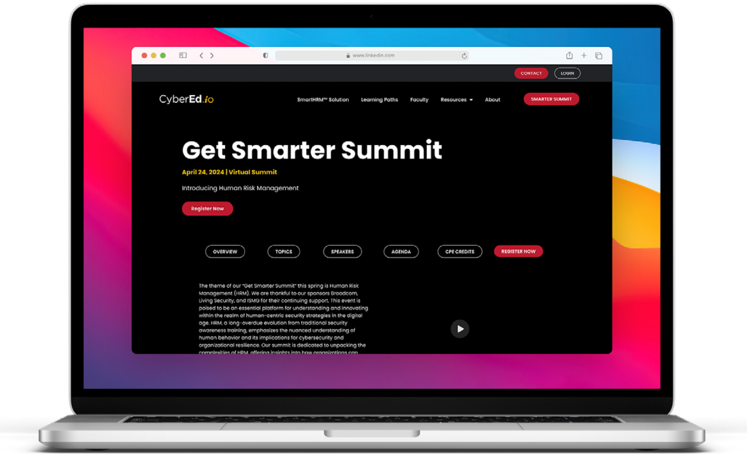
Gone are the days of conventional security awareness training. HRM represents a seismic evolution into the intricate realm of human behavior and its profound implications for cybersecurity and organizational resilience. It's not just about recognizing threats. It's about understanding the human element within them.

The "Get Smarter Summit" will drill into unraveling the complexities of HRM. Through dynamic discussions, thought-provoking panels, and innovative workshops, our aim is to equip you with the insights and strategies needed to anticipate, mitigate, and manage human-related risks effectively.

This isn't just another technology event. It's a rallying call for leaders, innovators, and thinkers alike to unite in forging a path to safer, more resilient organizations. Join us to help catalyze change and shape the future of cybersecurity together.

Register now to secure your spot in this pivotal conversation. Don't miss out on this opportunity to be part of a movement that's redefining cybersecurity and securing our digital future.

Register Now



Get Smarter Summit

April 24, 2024 | Virtual Summit

Introducing Human Risk Management

The theme of our "Get Smarter Summit" this spring is Human Risk Management (HRM). We are thankful to our sponsors Broadcom, Living Security, and ISMG for their continuing support. This event is poised to be an essential platform for understanding and innovating within the realm of human-centric security strategies in the digital age. HRM, a long-overdue evolution from traditional security awareness training, emphasizes the nuanced understanding of human behavior and its implications for cybersecurity and organizational resilience. Our summit is dedicated to unpacking the complexities of HRM, offering insights into how organizations can

CIO BUSINESS TRANSFORMATION AWARDS & SUMMIT '24
Brought to you by CIO.inc
Every connection counts
We need a different approach

Source: CIO Business Transformation Awards & Summit 2024

INAUGURAL CIO AWARDS AND SUMMIT CELEBRATES INNOVATION AND TRANSFORMATION

The inaugural CIO Business Transformation Awards and Summit, held March 13, 2024, in New Delhi, India, united technology enthusiasts, business leaders and industry, to recognize the remarkable strides CIOs have made in business transformation.

The Information Security Media Group (ISMG) event, hosted by CIO.inc, catered to the modern CIO whose role has evolved beyond traditional boundaries to become instrumental in driving digital innovation across various domains, including supply chain, manufacturing, customer experience, and employee productivity.

Under a theme of "Business Transformation 2.0: CIO as a Catalyst of Change," the summit included critical discussions on topics such as the impact of artificial intelligence on business growth and the imperative need for re-skilling to adopt frontier technologies. Industry experts at the summit included:

- Neena Pahuja, executive member, National Council for Vocational Education and Training;
- Sumit Bhatia, director of information technology, InsuranceDekho;

- Rajesh Kumar, technology head, enterprise and government, India and SAARC, Juniper Networks;
- Atul Govil, chief transformation officer and head of SAP and IT, corporate, India Glycols Ltd.; and
- Sunil Pandey, senior vice president and CIO, HFCL Ltd.

The experts shared diverse perspectives from sectors such as banking, financial services, travel, manufacturing and healthcare. Speakers emphasized the need for aligning AI innovation with organizational goals and underscored the importance of adaptable data strategies in navigating the complexities of digital transformation.

The summit commenced with a keynote address by Sougat Chatterjee, executive director and CEO of Abhay Health, who stressed the significance of effective collaboration between CEOs and CIOs in shaping the future of technology adoption. Chatterjee highlighted the role of technology as a catalyst for establishing competitive advantage and market differentiation, emphasizing the CEO's expectations of the CIO in driving efficiency and stakeholder satisfaction.

AI emerged as a central theme in panel discussions, with experts debunking myths and exploring practical applications within enterprises. The importance of building an AI-ready culture and identifying genuine business needs for AI adoption was emphasized, alongside the necessity for alignment between CIOs and boards in fostering innovation while maintaining core business objectives.

Dr. Vinay Thakur, MD of the National Informatics Centre Services Inc. (NICSI), Ministry of Electronics and IT, Government of India, delivered a keynote address highlighting the importance of transformative digital projects in advancing e-Governance initiatives.

The summit concluded with the much-anticipated CIO Awards ceremony, recognizing visionaries in technology and business transformation. Attendees honored the nation's top C-suite executives with awards presented in various categories such as Visionary CISO, Woman Leader in Security, Patented Projects, and Lifetime Achievement.

The awards program, overseen by a distinguished jury panel, celebrated the contributions of tech leaders in driving industry-wide innovation and transformation. Overall, the CIO Business Transformation Awards and Summit set a new standard for knowledge sharing and recognition of excellence in driving digital innovation.

Source: CIO Business Transformation Awards & Summit 2024

AI and the Art of Cyber Defense

Insights from Sam and Red Curry

In today's fast-paced digital world, cybersecurity serves as a reliable shield, safeguarding the integrity, confidentiality, and availability of personal and organizational information. But as digital threats grow wilier, it's increasingly clear that our traditional defenses are not keeping up with the pace of change.

This is where Artificial Intelligence (AI) is well-positioned to tilt the balance – some might say for the first time – in favor of cyber defenders. Leading the charge in this mission are Sam and Red Curry, who are experts in cybersecurity and pioneers in melding AI into current cybersecurity practices.

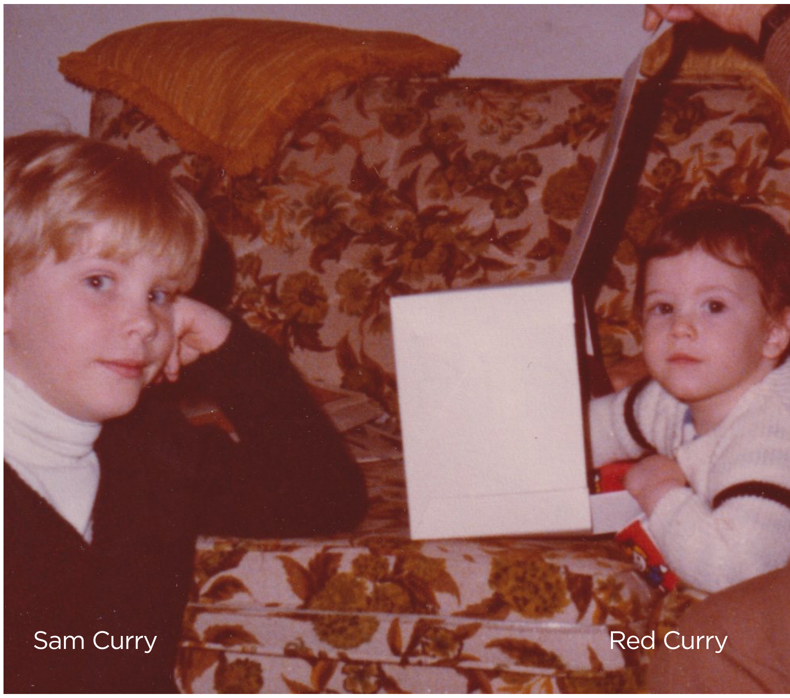
Both gentlemen generously agreed to sit for an interview with CyberEd Magazine to help explain how AI is enhancing cybersecurity in 2024, shedding light on our best path forward, given the complexities and ethical challenges that arise in this technological partnership. Their valuable insights show the promise and intricacies inherent at the intersection of AI and cybersecurity, reminding us to keep moving, carefully, forward.

UNDERSTANDING AI'S CYBERSECURITY POTENTIAL

Can you elaborate on specific ways AI is reshaping defensive strategies?

Sam Curry: AI is not just changing the game. It's rewriting the rules of cybersecurity. By employing predictive analytics, AI allows us to move from a reactive to a proactive stance, foreseeing threats before they manifest. Imagine a system that analyzes patterns from past cyber incidents globally and identifies a seemingly benign activity on your network as the precursor to a sophisticated attack. Before the threat materializes, AI-driven tools can automatically isolate the affected network segment and alert human analysts for further investigation, effectively preventing a potential breach. This anticipatory approach means we're not just waiting for attacks to happen, we're preventing them in advance. And we know that reducing the attack surface now with a zero trust architectural approach will help future-proof us against unforeseen and innovative attack vectors in an age of AI-assisted cyber offense.

Red Curry: Also, AI's ability to process information at a speed and scale unimaginable to humans transforms threat detection. We're now capable of digesting and analyzing data from countless sources instantly, enabling us to spot anomalies and potential threats with a precision and efficiency that were previously unattainable.


Sam Curry

Red Curry

What are the biggest risks of using AI in cyberattacks?

Red Curry: The most significant risks lie in the domains of misinformation and disinformation. Given its persuasive capabilities, AI can fabricate content that's indistinguishable from reality, leading to widespread misinformation. This is particularly concerning in sensitive periods like during this election year, because the integrity of information is threatened by threat actors.

Sam Curry: The immediate future shows a proliferation of offensive uses of AI in cyberattacks, which poses a real threat. However, the landscape is poised to change. I believe the scale will tip in favor of defense as we refine AI technologies and focus on developing robust defensive AI systems that can counteract these offensive tactics.

Please explain when and how the balance may shift in favor of defense, and what catalysts you foresee in this shift?

Sam Curry: The shift towards defense will be gradual and is contingent upon our approach to integrating AI within our ethical and operational frameworks. As we become more adept at leveraging AI for defensive purposes and establish rigorous ethical standards for its use, we'll see a natural progression towards a more secure cyber environment. The key catalyst for this shift will be our collective ability to innovate responsibly and ensure that AI technologies are developed and deployed with a clear understanding of their impact.

Red Curry: This transition to a defense-dominant landscape will also depend on our commitment to vigilance and responsibility. As cybersecurity professionals, we must be proactive in identifying potential vulnerabilities that AI might introduce and work tirelessly to mitigate these risks. The catalyst for change will be a combination of technological advancement, ethical guidance, and human insight, leading to a future where AI serves as a pillar of our cybersecurity defenses rather than a weapon against us.

Red Curry

Sam Curry

How do AI-driven predictive analytics change cyber defense planning?

Sam Curry: Predictive analytics revolutionize our defensive strategy by not just reacting to threats as they occur but by forecasting potential vulnerabilities and thwarting attacks before they materialize. This shift to a more anticipatory defense posture fundamentally changes how we secure our digital assets.

RESHAPING CYBERSECURITY TRAINING USING AI

Traditional cybersecurity education has often been criticized for its lag in catching up with real-world challenges. Courses can be overly theoretical, lacking the hands-on experience crucial for understanding the dynamic and fast-paced nature of cyber threats. AI is generating a seismic shift not only with the advent of more advanced defensive tools but also in fundamentally altering how future professionals are educated and trained.

What is the current state of cybersecurity education, and in what ways does AI alter this view?

Sam Curry: We're at a crossroads in cybersecurity education. Traditional models are struggling to equip students for the modern cyber battleground. AI introduces a dynamic shift, transforming static, theory-heavy curricula into vibrant, practical learning experiences.

Red Curry: We envision a future where AI not only complements but significantly enhances cybersecurity education from the ground up, starting as early as kindergarten. It's about creating a foundation that's as much about understanding the digital world as it is about reading and writing.

Why is training so important for using AI in cybersecurity and what key areas should this training focus on?

Red Curry: Training with AI in cybersecurity is pivotal. It's not just about simulating attacks but about building a nuanced understanding of AI's capabilities and limitations. Focus areas should include AI-driven threat modeling, data analysis, and the development of ethical hacking skills, all within AI-enhanced environments.

Sam Curry: Also, training should emphasize interdisciplinary skills. AI's impact on cybersecurity isn't isolated; it intersects with legal, ethical, and policy domains. Preparing students for this reality is essential.

AI'S ROLE IN CYBERSECURITY EDUCATION

What are the ethical implications of integrating AI into cybersecurity education and how can cybersecurity teams foster an ethical AI culture?

Sam Curry: The ethical challenges are as crucial as the technical ones. Integrating AI into education brings about questions of bias, privacy, and the moral implications of AI-driven decisions. Our curriculum must address these head-on, preparing students to navigate these complex issues.

Red Curry: Indeed, ethical training in AI use should be core, not peripheral. We advocate for a curriculum that fosters critical thinking about the consequences of technology, encouraging a future where cybersecurity professionals are not just technically proficient but also ethically grounded. Fostering an ethical AI culture requires organizations to prioritize training that encompasses the ethical use of AI, including understanding bias, privacy implications, and the broader societal impacts. Regular ethical audits of AI systems and decision-making frameworks that include ethical considerations can also help.

In what ways will AI impact the future of cybersecurity education?

Red Curry: AI's impact will be transformative, driving a shift toward continuous, adaptive learning environments. Collaboration across sectors will be key to this evolution, ensuring

A third Curry brother, Ben (right), with Sam (middle) and Red (left).

education stays aligned with industry needs and innovations. To illustrate the concept of adaptive learning, if an AI observes a new malware strain bypassing existing defenses, it analyzes the attack vector, updates its threat detection models accordingly, and immunizes the system against similar future attacks. This continuous learning process ensures that cybersecurity defenses evolve in tandem with threats.

Sam Curry: The pace of change in cybersecurity means education can't stand still. AI facilitates the expansion of lifelong learning, ensuring that tomorrow's professionals remain adept and agile, capable of responding to emerging threats with confidence and ethical clarity.

What other impacts will AI have on cybersecurity education?

Red Curry: Beyond the technical training needed, AI will democratize access to cybersecurity education, breaking down barriers related to geography, background, and prior knowledge. It opens up pathways for a diverse new generation of cybersecurity talent, equipped to tackle the digital challenges of the future.

Sam Curry: The renaissance in cybersecurity education, spurred by AI, might well extend into the liberal arts, encouraging a broader understanding of technology's role in society. It's about fostering a holistic view where technology serves humanity, guided by a strong ethical compass. This isn't about replacing traditional learning paths but enriching them. By weaving AI and cybersecurity principles into the fabric of liberal arts education, we encourage a broader understanding of how technology shapes our culture, ethics, and daily lives… Consider the implications of AI on privacy, freedom of speech, and even democracy itself. These are not merely technical challenges but societal ones. A student studying philosophy, history, or literature should grapple with these issues just as much as someone in a computer science lab. This interdisciplinary approach ensures that our future leaders, regardless of their field, are equipped with a nuanced understanding of technology's role and responsibilities in society.

Red Curry: Encouraging students to engage with ethical dilemmas, understand the biases inherent in AI systems, and the potential for both positive and negative impacts on society fosters a generation of technologists and non-technologists alike who are ethically aware and engaged…Imagine a curriculum where a cybersecurity course includes literature on science fiction's predictions of technology's future, or where computer science students are required to take ethics classes that explore the moral quandaries of AI. This is the kind of interdisciplinary education that can prepare students for the complexities of a world where technology is inextricably linked with every aspect of our lives.

Sam Curry: We need to dismantle the silos that have traditionally separated STEM fields from the liberal arts. The future of cybersecurity, propelled by AI, depends on our ability to foster a holistic educational ecosystem. It's about creating a dialogue between technology and humanity, ensuring that as we advance, we do so with a guiding ethical compass and a profound understanding of our societal responsibilities.

NAVIGATING THE FUTURE OF AI IN CYBERSECURITY

The integration of AI into defense mechanisms and threat detection systems is reshaping our approach to digital security. Sam and Red Curry have been at the forefront of advocating for AI's potential to enhance cybersecurity efforts. Their insights, alongside broader industry trends, suggest a future where AI is integral to cybersecurity strategies.

Please expand on coming AI-driven threats and opportunities.

Sam Curry: AI's potential to revolutionize cybersecurity practices and the emergence of AI-powered threats brings unprecedented opportunities for defense, automating responses at a speed and scale that humans alone cannot achieve. For example, an AI system that continuously monitors network traffic may identify a pattern matching ransomware dissemination behavior within milliseconds of its occurrence. The AI system then triggers automated countermeasures, such as blocking the source IP and quarantining affected files, long before the malware can encrypt critical data. On the flip side, AI also opens new avenues for adversaries. As we innovate, so do our adversaries. The race doesn't end, it evolves, as we leverage AI to strengthen defenses. That's also when we inadvertently provide a playbook for attackers to enhance their offensive capabilities.

Red Curry: AI's adaptability is also its greatest strength. While it empowers cybersecurity systems to detect and neutralize threats with unprecedented efficiency, it also raises concerns about the automation of attacks and the potential for misuse. And the potential for AI to autonomize attack strategies raises the stakes. It's imperative that as we harness this power, we also implement robust ethical frameworks and maintain vigilant oversight to prevent misuse.

What strategies would you recommend for organizations to balance AI capabilities with human judgment in their cybersecurity initiatives?

Sam Curry: Integrating AI into cybersecurity isn't about replacing human judgment but augmenting it. Organizations should rigorously evaluate AI solutions, ensuring they align with ethical standards and complement the expertise of cybersecurity professionals.

Red Curry: The key is in creating a symbiotic relationship where AI enhances human decision-making, not supplants it. By establishing clear protocols for AI intervention, conducting regular reviews of AI decisions, and fostering a culture of ethical AI use, we can achieve a balanced cybersecurity posture.

When integrating AI into cybersecurity efforts, how do you navigate the balance between improving security and upholding individual privacy?

Sam Curry: Balancing privacy and security is a particularly nuanced challenge. AI's ability to analyze vast datasets can significantly improve threat detection. But it also raises valid concerns about privacy, as the collection and analysis of data must always respect individual rights and comply with regulatory standards. We must ensure AI systems are designed and operated within a framework that prioritizes data minimization and transparency. For instance, when an AI system identifies a potential threat based on user behavior patterns, the specifics of how it processes personal data to make that determination should be transparent and align with privacy-preserving principles.

Red Curry: The question of privacy versus security isn't a zero-sum game. Ethical AI use in cybersecurity means deploying AI in a way that both protects digital assets and respects individual privacy. This involves implementing robust data anonymization techniques and ensuring AI algorithms are trained on data that's been collected and processed in line with strict privacy standards. There's also a need for ongoing

Sam Curry and Tom Field at RSAC 2020.

dialogue with stakeholders, including privacy advocates, to continuously adjust approaches. An example of balancing these considerations is the deployment of AI in network monitoring. Although AI can scrutinize network traffic for signs of malicious activity, it should do so in a way that abstracts individual identities, focusing on behavior patterns rather than personal data.

AI'S FUTURE ROLE IN EDUCATION AND GLOBAL AFFAIRS

Please describe AI's future role in education and continuous training?

Red Curry: The transformative potential of AI in cybersecurity education underscores the necessity for robust education and continuous training programs. By incorporating AI into training programs, we can create more dynamic, realistic, and engaging learning experiences. We will need professionals who are not only technologically proficient but also ethically aware and adaptable. An approach that incorporates real-time simulations, AI ethics, and hands-on experience with the latest AI tools and technologies will help equip professionals with the technical skills as well as a deeper understanding of the ethical dimensions of AI use in cybersecurity.

Sam Curry: Continuous education is paramount. The future of AI and cybersecurity hinges on fostering a culture of lifelong learning among professionals. The rapid pace of technological change necessitates an ongoing commitment to education, ensuring that skills and knowledge remain relevant. Continuous training programs, industry certifications, and higher education courses must evolve in tandem with technological advancements, empowering professionals to navigate the complexities of AI-driven cybersecurity. Beyond a subject of study AI must facilitate ongoing learning to help us ensure cybersecurity professionals can adapt to the evolving threat landscape.

How do you foresee AI shaping the cybersecurity workforce of the future?

Sam Curry: AI is set to revolutionize the cybersecurity workforce by demanding a new breed of professionals. We'll see roles that blend AI knowledge with cybersecurity expertise, requiring continuous upskilling and a flexible mindset to adapt to new threats and technologies.

Red Curry: Yes, and because AI will democratize cybersecurity knowledge, making it accessible to a broader audience, this inclusivity could lead to a more diverse cybersecurity workforce, equipped with a wider range of perspectives and solutions to tackle complex digital threats.

Please discuss the role of global collaboration in harnessing AI for cybersecurity, especially in terms of cyber warfare and national security?

Sam Curry: As cyber threats transcend national boundaries, a unified global effort becomes essential to develop standards and share knowledge. We know no nation stands alone. The global nature of cyber threats necessitates international collaboration. By sharing insights, best practices, and research on AI's application in cybersecurity, we can collectively enhance our defenses and develop norms that govern AI use in cyber warfare and national security.

Sam Curry and Sanjay Kalra

Red Curry: Anticipating the future, we see an intensifying arms race powered by AI. To counter this, our approach must become more proactive, grounded in international cooperation and continuous education. The journey ahead requires vigilance, ethical consideration, and an unwavering commitment to continuous learning. In many ways, the role of education becomes not just a foundation but a continuous beacon guiding us through the complexities of AI in cybersecurity to help forge a more secure digital world.

A FEW FINAL THOUGHTS

When integrating AI into cybersecurity, we'll all need to be mindful of the critical balance between innovation and ethics, the transformative potential of AI in education, and the paramount importance of global collaboration and continuous learning.

Moving forward, our greatest strength lies in our ability to blend technological advances into the rich tapestry of human values. As we work to harness the power of AI to secure our digital frontier, it's crucial to ensure that as we advance, we remain steadfast in our commitment to protecting not just our digital assets, but the very fabric of our society.

In the words of Sam and Red Curry, the journey ahead is both challenging and promising. We'll need vigilance, integrity, and an unwavering dedication to the betterment of humanity to get this right. Hanging in the balance of AI's capabilities and our ethical imperatives lies the key to a safer, more secure digital world for all.

Sam Curry (left) and Red Curry (right)

The Evolution of Integrated Threat Detection and Response (ITDR)

Highlights from CyberEd's Latest Research Report

Facing increasingly sophisticated cyber threats, organizations are in search of robust and efficient cybersecurity solutions.

Managed Detection and Response (MDR) and **Extended Detection and Response (XDR)** are considered frontrunners in providing threat detection and response capabilities. However, the arrival of ITDR now offers an advanced technological approach that integrates AI and machine learning (ML) with predictive analytics. To fully grasp the concept of ITDR it's important to understand MDR and XDR.

1. **Managed Detection and Response (MDR)** offers organizations a team of cybersecurity experts who continuously monitor and manage security threats using a combination of best-of-breed loosely integrated point solutions. MDR's focus is on detecting and responding to threats using a combination of technology and human expertise.
2. **Extended Detection and Response (XDR)** builds on MDR by integrating security products across layers, including networks, cloud services and endpoints. By correlating data from security domains, XDR aims to provide a comprehensive view of the threat landscape. Now, the emergence of ITDR combines the strengths of MDR and XDR while introducing predictive analytics, AI and ML as key differentiators.
3. **Holistic Integration —** ITDR seamlessly integrates technologies, processes and human expertise across IT domains. This integration creates a platform for threat detection, analysis and response
4. **Advanced Analytics and AI —** ITDR takes advantage of cutting-edge analytics and artificial intelligence to enhance threat detection by harnessing the power of intelligence and advanced learning. ITDR can anticipate and proactively address

security incidents, which goes beyond the reactive approaches commonly seen in MDR and XDR.

MORE DATA, FASTER KNOWLEDGE, BETTER DECISIONS

One key aspect that sets ITDR apart is its integration of automation, which not only provides response mechanisms, like MDR and XDR but also ensures faster and more efficient response actions. This helps to minimize vulnerability windows and mitigate the impact of security breaches.

A distinguishing feature of ITDR is its capability to seamlessly integrate cybersecurity tools and IT management systems into a unified platform. This integration extends across network security, endpoint protection, cloud security, identity, applications and devices to build a more complete view of an organization's security posture.

ITDR also excels at data aggregation by collecting information from sources such as post-control data from SIEMs (Security Information and Event Management) IDS/IPS systems (Intrusion Detection/Prevention Systems) firewalls and endpoint protection platforms. This data is then correlated to identify patterns and anomalies that may signal cyber threats. To detect threats that traditional rule-based systems might overlook, ITDR employs AI algorithms to continuously learn from data and behaviors, enhancing its capabilities over time. When a threat is detected by an ITDR, it can initiate automated response protocols without delay or human intervention. These actions involve isolating systems, implementing updates or adjusting firewall rules without the need for human intervention.

ITDR VS MDR

In comparing ITDR with MDR and XDR, this report found the scope of protection differs between MDR, XDR and ITDR. While MDR focuses on detection and response and XDR extends this to security domains, ITDR offers a comprehensive approach. It not only covers detection and response. It

also includes prevention and prediction capabilities, addressing a wider range of potential security incidents.

BUILDING A STRONGER SECURITY POSTURE

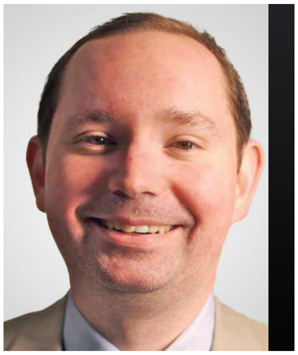
Integration and correlation play roles in both XDR and ITDR. However, ITDR takes it a step further by integrating not just security tools, but also incorporating IT management and compliance frameworks. This holistic integration creates a next-gen security posture. Automation is essential in both MDR and XDR operations as they involve intervention.

However, ITDR leverages advanced automation capabilities to minimize hands-on intervention. This leads to more and better threat management. Unlike MDR and XDR that primarily rely on reactive measures, ITDR goes beyond that by utilizing analytics to forecast and neutralize threats before they manifest. This proactive approach is crucial in combating threats (APTs) and zero-day exploits.

Ultimately, ITDR represents the next phase in the advancement of cybersecurity solutions. Its integrated approach combining the strengths of MDR and XDR with cutting edge technologies and methodologies makes it a powerful weapon against cyber threats now and in the future.

Please visit CyberEd's website to download the full report here.

CyberEd Featured Faculty



George Finney

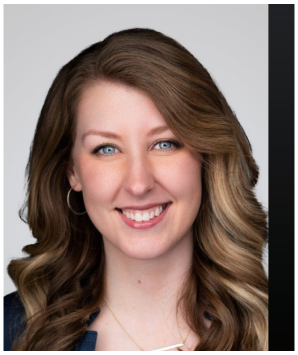
Chief Security Officer and Director of Digital Interests,
Southern Methodist University

As chief security officer for Southern Methodist University, George is an early Zero Trust advocate and an expert on policy, awareness, compliance, operational management and the complex legal issues surrounding modern information security. He's also a best-selling cybersecurity, including the award-winning book, Well Aware: Master the Nine Cybersecurity Habits to Protect Your Future.

Sam Curry

VP, CISO, Zscaler

Sam Curry is a 30-year veteran who worked at Signal 9 Solutions, a start-up that invented the personal firewall, deployed the first commercial implementation of Blowfish, and devised early stealthy (symmetric key) VPN technology, which was later sold to McAfee. Curry went on to serve as Chief Security Architect and as head of Product for McAfee.com, before moving to leadership roles at RSA, including head of RSA labs at MIT and head of product, CTO, and Distinguished Engineer for EMC. After seven years with RSA, Curry served as SVP and CISO at MicroStrategy, then as CSO and CTO for Arbor Networks before it became Netscout, and later as CSO for Cybereason.



Kelly Hood

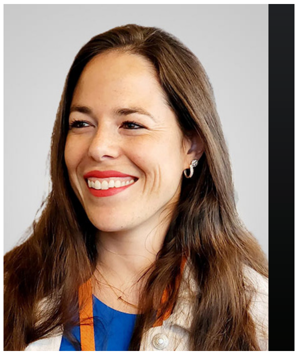
EVP and Cybersecurity Engineer, Optic Cyber Solutions

Kelly Hood is an EVP and cybersecurity engineering expert supporting organizations across sectors to develop and implement strategies to manage cybersecurity and privacy risks. 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.

Jimmy Mesta

Chief Technology Officer, KSOC

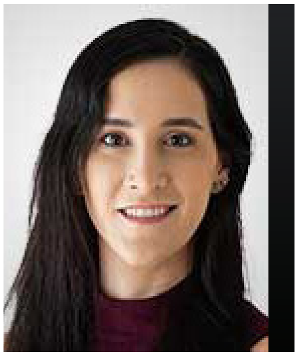
Jimmy Mesta is the founder and Chief Technology Officer at KSOC, the organization that triages risk across Kubernetes clusters in real time. He is responsible for the technological vision for the KSOC platform. Mesta, veteran security engineering leader focused on building cloud-native security solutions, 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.



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.



Nikki Robinson

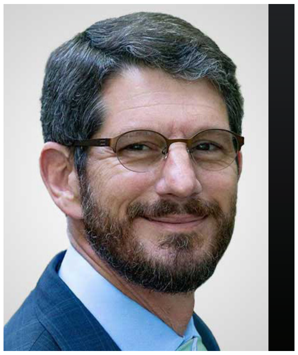
STSM - Cyber Resiliency and Recovery, IBM

Dr. Nikki Robinson is a senior IBM Cybersecurity Engineer with 15+ years of experience in the IT and cybersecurity fields. Skilled in statistical data analysis, team leadership, penetration testing, and risk management, Nikki earned her doctorate in Cybersecurity from Capitol Technology University. Dr. Robinson is certified as a CISSP and CEH and is a member of the Board of Directors for InfraGard Maryland Chapter and provides support for InfraGard at the national level on the Journal Review Committee. Nikki teaches graduate-level courses in Quantitative Methods, Incident Response, and Healthcare Mobile Device Security at Touro College and Capitol Technology University.

Char Sample

Cybersecurity researcher, ICF

Dr. Char Sample is a cybersecurity researcher at ICF with decades of experience. Dr. Sample currently supports NSF research initiatives in Computer and Network Science research. Dr. Sample's current research focuses on deception, and the role of cultural values in cybersecurity events and decision-making. One other area of research that she finds interesting is the relationship between human cognition and machines. Currently, Dr. Sample is continuing research on modeling cyber behaviors by culture, data resilience, cyber-physical systems and industrial control systems and trustworthy artificial intelligence (TAI).



Grant Schneider

Senior Director of Cybersecurity Services, Venable LLP

Grant is a recognized leader in the cybersecurity sector with extensive experience driving organizational change, developing policy and governance structures, and driving technology modernization initiatives. Having served as the U.S. federal chief information security officer (CISO) for the White House, and on the White House National Security Council (NSC) staff as a special assistant to the President and senior director for cybersecurity policy, and as the Defense Intelligence Agency chief information officer (CIO), Grant is uniquely positioned to assist global technology clients with navigating strategic, operational, and risk management needs.

Dom Lombardi

CYBERSECURITY INSIGHTS PODCAST

Collaborative Security: The Team Sport Approach

Dom Lombardi is the vice president of security and trust at Kandji, where his team is responsible for technical operations, information security, security risk, data privacy, and compliance. Prior to Kandji, Dom built risk-based security, technology, and privacy programs at Klaviyo, Kyruus Health, and Barton Associates. Leveraging his expertise in product-led hyper-growth and quantitative security risk management, Dom has created several SaaS-specific, engineering-focused programs to secure fast-paced modern environments.

In this episode of Cybersecurity Insights, Dom discussed:

- Emphasizing security as a collaborative effort among teams;
- Examining different working styles and their implications for device security;
- Exploring the phenomenon of passkeys and their significance in authentication;
- And much more.

Learn more by listening to the podcast here.

Lotem Guy

CYBERSECURITY INSIGHTS PODCAST

Securing Applications and Managing Attack Surfaces

Lotem Guy is the VP of product at Cycode. He is also a security researcher and developer with more than 15 years of experience in the tech industry. Lotem's areas of expertise include application security, cloud security, endpoint security and ethical hacking. He holds a master's degree in computational biology, blending unique analytical skills with cybersecurity expertise. Throughout his career, he has contributed to numerous innovative security solutions, navigating complex challenges in the evolving landscape of cybersecurity.

In this episode of Cybersecurity Insights, Lotem discussed:

- Enhancing application security measures;
- Mitigating risks associated with unmanaged attack surfaces;
- Exploring the principle of "shift left" in cybersecurity practices;
- And much more.

Learn more by listening to the podcast here.

Galit Lubetzky Sharon

CYBERSECURITY INSIGHTS PODCAST

What Risk/Compliance Leaders Overlook in Security

Galit Lubetzky Sharon is a retired colonel from the prestigious Unit 8200. She has vast, hands-on experience designing, developing and deploying some of the Israeli Defense Forces' (IDF) most vital defensive and offensive cyber platforms, as well as leading large development teams. Galit was an integral part of developing the IDF's first cyber capabilities and continued improving and enhancing these capabilities throughout her military career. She is the recipient of numerous accolades, including the prestigious Israeli Defense Award. Galit co-founded Wing Security and is its chief executive officer

In this episode of Cybersecurity Insights, Galit discussed:

- The current state of compliance processes;
- Under- and over-explored security areas;
- Key compliance challenges identified by Wing Security;
- And much more.

Learn more by listening to the podcast here.

Jared Atkinson

CYBERSECURITY INSIGHTS PODCAST

The Next Frontier in Purple Teaming

Jared is a security researcher with a specialization in digital forensics and incident response. Recently, he has been building and leading private sector hunt operations. Prior to this, Jared led incident response missions for the U.S. Air Force Hunt Team, detecting and mitigating advanced persistent threats across Air Force and Department of Defense (DoD) networks. With an expertise in PowerShell and the open-source community, he is also the lead developer of PowerForensics and Uproot and maintains a DFIR-focused blog.

In this episode of Cybersecurity Insights, Jared talks about:

- Red team assessments;
- Evaluating purple team exercises and assessments in their present state;
- Advocating for a refined method focusing on testing attack techniques;
- And much more.

Learn more by listening to the podcast here.

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

Risk Analysis Warrior

- Authorization Fundamentals
- Enterprise Security Risk Management
- Vulnerability Assessments
- Developing Secure Code
- NIST DoD RMF
- NIST Cybersecurity Framework
- NIST Cybersecurity Framework Project

Learning Path Spotlights

CyberEd.io provides foundational technical training for Cyber-Warriors seeking education and employment in detection, defense, and protection. We strive to instill understanding about why reasoning matters, why adaptability matters, why thinking like hackers matters. We help students build a culture of cybersecurity and an appetite for continuous learning. In this issue, we highlight two Cyber-Warrior Learning Paths:

- ICS/OT Security Warrior
- Risk Analysis Warrior

ISC/OT Security Warrior

An Industrial Control Systems (ICS)/Operational Technology (OT) Cyber-Warrior helps safeguard critical infrastructure from cyber threats. They protect industrial control systems, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other OT components from cyberattacks that could disrupt essential services or cause damage to infrastructure and public safety.

ICS cyber warriors require a strong foundation in cybersecurity principles, networking, and system administration. They value and pursue certifications, including: Certified Information Systems Security Professional (CISSP); Certified Ethical Hacker (CEH); Certified SCADA Security Architect (CSSA); and GIAC Industrial Cyber Security Professional (GICSP).

Our curriculum provides specialized training programs and courses focused on ICS cybersecurity, covering topics such as risk assessment, penetration testing, incident response, and secure coding practices tailored to industrial environments

Risk Analysis Warrior

CyberEd views Risk Analysis Warriors as professionals responsible for identifying, assessing, and mitigating risks within an organization. They analyze various risks, including financial, operational, strategic, and cybersecurity risks, to help organizations make informed decisions to protect their assets.

Risk Analysis Warriors identify, assess and develop risk mitigation strategies and action plans to address identified risks. This may involve implementing controls, safeguards, or risk transfer mechanisms to reduce the likelihood or severity of risk events and their potential consequences. They also monitor the effectiveness of risk mitigation measures. They also report risks to key stakeholders and help develop and implement risk management policies, procedures, and frameworks.

Typically, Risk Analysis Warriors hold a bachelor's or master's degree in finance, economics, business administration, accounting, risk management, or a related discipline. Key risk management certifications they strive for include: Certified Risk Analyst (CRA); Financial Risk Manager (FRM); Chartered Financial Analyst (CFA); Certified Information Systems Auditor (CISA); and Certified in Risk and Information Systems Control (CRISC).

+1-609-356-1499 • info@cybered.io • www.cybered.io

CyberEd
MAGAZINE