EC-Council C|EH

# THREAT REPORT 2024

UNVEILING THE ACTUAL STATE OF AFFAIRS DIRECTLY FROM THE FRONT LINES OF CYBERSECURITY

## CYBERSECURITY IN THE ERA OF AI

AI ENABLED THREAT ACTORS VS CYBERSECURITY DEFENDERS

- 20 VITAL STATS WITH TECHNICAL INSIGHTS
- LEARN THE TOP 5 IoCS
- 83% OF PROFESSIONALS AFFIRM A RAPID EVOLUTION OF ATTACKS WITH AI
- 80% USED MULTI-FACTOR AUTHENTICATION TO MITIGATE RISKS ASSOCIATED WITH THE TOP 5 CLOUD TTPS

# **Table of** Contents:

# 1 Executive Summary

Cybersecurity threats and the challenge of finding skilled professionals to defend networks are major concerns and fears for many organizations. As of 2023, there is a global shortage of skilled cybersecurity professionals to fill critical organizational roles.[1] Adversaries and threat actors are aware of this threat. They will find ways to continue penetrating networks and retrieving information critical to national security or sensitive and classified information for financial gains. External threats are a concern; however, many attacks come from internal sources. Some attacks are intentional, while others are due to a lack of training and awareness. Due to the high volume of threats and attacks, in 2021, US President Joe Biden signed an Executive Order on Cybersecurity to modernize cybersecurity defenses.[2] In 2022, President Biden signed the Strengthening American Cybersecurity Act.[3] This law established (1) an interagency council to standardize federal reporting of cybersecurity threats, (2) a task force on ransomware attacks, and (3) a pilot program to identify information systems vulnerable to such attacks. The focus is to strengthen the federal cyber workforce and foster collaboration across all levels of government, specifically to "improve collaboration, share security tools, procedures, and information more easily." For each organization, the responsibility of maintaining secure networks while protecting sensitive information is of the highest priority, and proper planning and assessments are essential to reduce the risks of attacks. This EC-Council Threat Report 2023 includes research data regarding cyber threats and concerns about artificial intelligence (AI) It provides different methods for detection and mitigation from experienced IT and cybersecurity professionals.

**Steve Graham**

**Senior Vice President | EC-Council**

## Chairperson of C|EH Advisory Committee

Steven Graham is the Senior Vice President of EC-Council | Global, a world leader in cybersecurity education, training, and certification. Steve leads all divisions in North America, including Education Technologies, Partnership Strategies, Sales, Operations, and R&D. During his 16 years at EC-Council, Steve has served on the Executive Committee of the EC-Council Group, steering product, and technology strategies to enable education partners in over 140 countries to better transfer knowledge and skills to the evolving cybersecurity workforce. Since 2007, Steve has been the primary liaison to the US Department of Defense at EC-Council, helping shape policies and programs affecting the DoD Cybersecurity Workforce.

## Our special thanks to the Certified Ethical Hacker Advisory Board of Members who actively contributed to this Report:

**Irene Corpuz**

Manager, Projects-Strategy and Future Department Federal Education

**Lisa Bock**

Security Ambassador, Author, Speaker

**Claudio Cilli**

Cybersecurity and Intelligence researcher and advisor National Security and threat-intelligence

**Allen Dziwa**

Cyber Risk Specialist and SME Federal Reserve Bank of Cleveland

**Khasim Mirza**

Senior Principal IT Security Analyst Oracle

ORACLE

**Dr. Teju Oyewole**

Director, IT Security Sunwing Travel Group

sunwing

**Ken Underhill**

Executive Producer, Host, and Owner, Cyber Life

CYBER LIFE

**Daniel Paillet**

Cybersecurity Lead Architect, Schneider Electric

Schneider Electric

**Febin Prakash**

Assistant Professor of Cybersecurity and Cyber Forensics, Jain (Deemed-to-be University)

JGI JAIN

## Threat Report Leader Editor:

**Cassandra Pristas**

**Leader Cybersecurity Instructor-EC-Council**

**Information Professional Officer**

**United States Navy Reserves**

**Adjunct Professor**

**5 Master's Degrees**

**Several IT Certifications**

**Pursuing PhD in Education**

Cassandra Pristas is the Lead Cybersecurity Instructor with EC-Council. She has over 24 years of experience in the IT and security industry. She has worked in many industry roles, including cyber analyst, systems administration, networking, information assurance, knowledge management, and SharePoint. Her experience includes working for large DoD companies, Jacobs Technology, Harris and General Dynamics, and serving in the United States Naval Reserves information warfare community. She has managed and led cyber professionals working with cyber protection teams and has experience teaching a cybersecurity curriculum to cyber professionals for all branches of the military. She is a lieutenant commander assigned to the Navy Reserve Southcom Headquarters in Miami, Florida, and the Navy Information Operations Center in Pensacola, Florida. She has several master's degrees, including the MSA, MS, MSIT, and MSC, and several IT industry certifications, and she is currently pursuing her PhD. She is an adjunct professor at the University of West Florida, teaching intelligence analysis courses. Cassandra has published several articles for the CHIPS Department of the Navy's Information Technology Magazine.

## Threat Report Deputy Editor:

Dr. Meisam is a technical cybersecurity practitioner with solid expertise in providing strategies and technical directions, building new service/business lines, diverse teams, and capabilities. He has over 20 years of experience in information technology, with 16 years dedicated to cybersecurity in leadership and technical roles. In his current role as Executive Director of Cybersecurity at EC-Council Global Services (EGS), Meisam is leading, managing, and delivering a wide range of cybersecurity services to multi-national clients, mainly in red teaming, threat hunting, DFIR, cyber drill, compromise assessment, and penetration testing. He is a contributor to the MITRE D3FEND project, serves as a mentor at the Blue Team Village, and has been a featured speaker at numerous global events and conferences, including Defcon, BSides, Nanosec, and NASSCOM.

**Dr. Meisam Eslahi**

**Executive Director Cybersecurity – EC-Council Global Services**

C|CISO, E|CSA, C|EH, C|HFI, C|EH, OSCP, ISMS LA

# 2 Key Report Findings

**83%**

### A Shift In the Winds:

note tangible alterations in attack methodologies amidst the AI revolution.

**80%**

### Layered Defense:

employ multi-factor authentication to combat the Top 5 Cloud Threat Tactics and Procedures (TTPs).

**82%**

### Education's Edge:

champion regular training needed for incident response.

**Over 70%**

### Bypassing the Barricades:

identify social engineering and zero-day exploits as top threat vectors.

**68%**

### Zeroing In on Zero-Day:

stated these exploits as the utmost challenges.

**66%**

### AI Readiness:

admit being unprepared for AI cyber onslaughts.

## Top 3 Application Security Vulnerabilities

**Security Misconfiguration**

**Vulnerable and Outdated Components**

**Authentication and Session Management Issues**

# 3 Introduction

Today's threats are emerging with new tactics, tools, and methodologies. EC-Council's threat report provides insight into factors important to cybersecurity professionals and relevant to what is happening in the industry. Threats are real, and hackers are finding ways to penetrate networks and cause disruption among organizations. Our adversaries will continue to attack our networks and gather intelligence regarding our national security. In 2023, hackers from China breached the email accounts of several prominent US government employees in the State Department and the Department of Commerce through a vulnerability in Microsoft's email systems. [4] In early 2023, it was discovered that a North Korean hacking group had conducted an espionage campaign between August and November 2022, targeting the medical research, healthcare, and chemical engineering industries.[5] The threats and attacks are endless; however, the industry must also prepare for artificial intelligence to continue its evolution into the cyber world, creating more attacks and more work through automation and simple computations of an algorithm. The shortage of skilled cybersecurity professionals, increased attacks, and the use of artificial intelligence are raising doubts and fear in many organizations and cybersecurity professionals.

## The Survey Demographic:

EC-Council recently surveyed working professionals to share their thoughts and reflect on their experiences working in various industries.

**The following statistics represent these participants:**

**1066+** professionals across 14 industries.

**62** cybersecurity designations.

**Over 50%** of the respondents had 10 or more years of experience.

**Over 25%** had served in leadership and management roles.


Artificial intelligence (AI) has been around for over sixty years. It is changing how people live, organizations and educational systems operate and conduct business. According to the Council of Europe, "AI consists of a set of sciences, theories, and techniques that aim to imitate the cognitive abilities of a human being." [6] AI is still in the beginning stages; however, organizations need to be made more aware of AI's capabilities, limitations, and future direction.

# 4 How Attackers Exploit AI

Survey participants were asked about the potential risks associated with AI in cyber attacks.

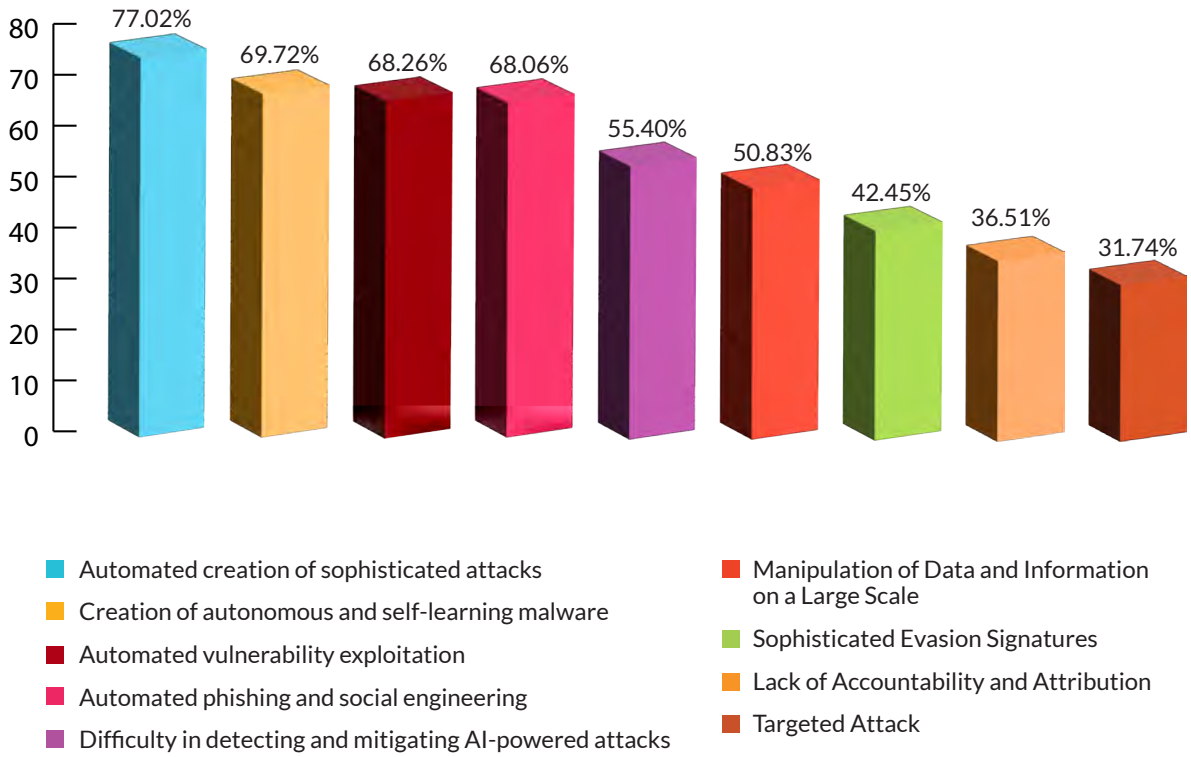
**The top 4 risks identified include the following:**

**Automated creation of sophisticated attacks**

**Creation of autonomous and self-learning malware**

**Automated vulnerability exploitation**

**Automated phishing and social engineering**



The automated creation of sophisticated attacks using AI is one of the top risks, mainly due to its mysterious nature and capabilities. As of today, there is no direct accountability for creating sophisticated attacks, nor are there real legal ramifications to creating the attacks. Artificial intelligence sees no ethical concerns and removes the human element of doing business and performing attacks.

The same concept applies to autonomous and self-learning malware. Companies need help to counteract malware that not only human attackers create but also AI. Moving forward, the concept of AI learning to create malware on its own and without any oversight can be highly alarming to cybersecurity professionals. Current tools that monitor and block malware attacks are more vulnerable to those created by AI. As the attacks become more sophisticated with various methodologies, algorithms, and exponential amounts of data, this concern can be overwhelming to counteract. Society and organizations are excited about using AI; however, creating self-learning malware can lead to more threats and attacks formulated by AI.

The use of automated phishing and social engineering is another concern about the application of AI. Phishing and social engineering are standard day-to-day threats for organizations across the globe. Individuals will be increasingly targeted through emails, telemarketing calls, and social media. According to Baker (2023), at IdentityIQ, AI can enable scammers to create highly realistic voice and speech synthesis via cloning scams, automate phishing campaigns, create fake videos, and manipulate social media platforms. [7] These attack strategies make it more challenging to differentiate what is real and what is not.

68% of respondents stated that AI's ability to automate vulnerability exploitation with phishing and social engineering is considered high risk to an organization. According to the Council of Europe, "automation remains far from human intelligence in the strict sense, which makes the name open to criticism by some experts." [8] The Council of Europe further notes, "The ultimate stage of their research (a "strong" AI, i.e., the ability to contextualize very different specialized problems autonomously) is not comparable to current achievements ("weak" or "moderate" AIs, extremely efficient in their training fields)." [9] However, in the future, there is no way to determine the limitations of using AI as more data is produced and shared on the internet.

# 5 How Defenders Use AI

Cyber attacks are evolving and becoming more prevalent around the world. Organizations cannot handle the number of attacks today, especially with the shortage of skilled cybersecurity professionals. If organizations have the right number of security professionals trained and prepared to help counter those attacks, they will be better off. However, as simple as this sounds, it takes work. In cybersecurity, "the lack of security skills in the IT industry is partly due to professionals working long hours and requiring patience, resources, knowledge, and experience." [10]

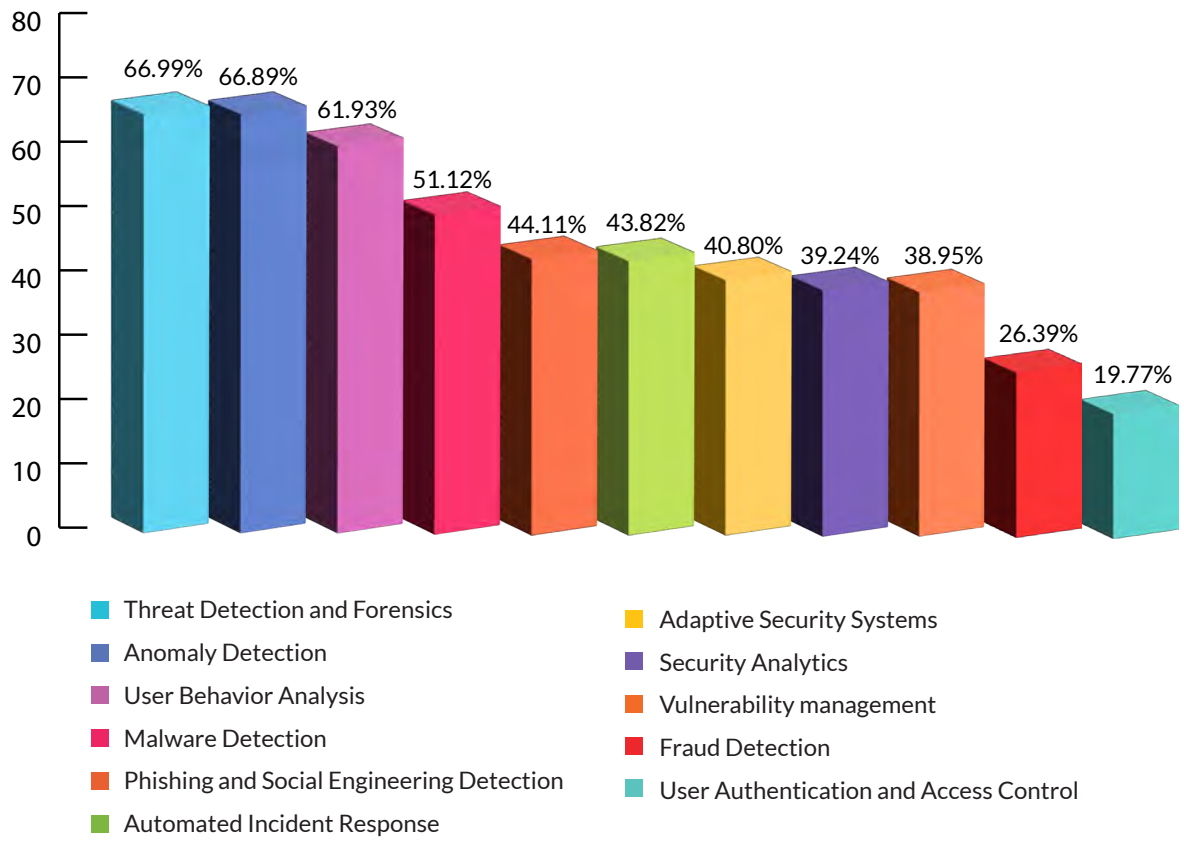
However, on the positive side, AI can provide benefits to address the needs of the cyber workforce shortage. Smith (2018) notes that using AI and automation can relieve some of the pressures that IT and cybersecurity professionals face. Some examples include "automating the longwinded and repetitive tasks that fill the workflows of IT teams, such as testing, basis threat analysis, and data deception tactics." [11] Using AI to help automate specific tasks can be an advantage in reducing the amount of time and resources for cyber professionals.

**During a recent survey, respondents were asked how AI/machine learning can help an organization's cybersecurity posture. Here are some of the findings:**

**67%** state that AI applications would help with threat detection and forensics.

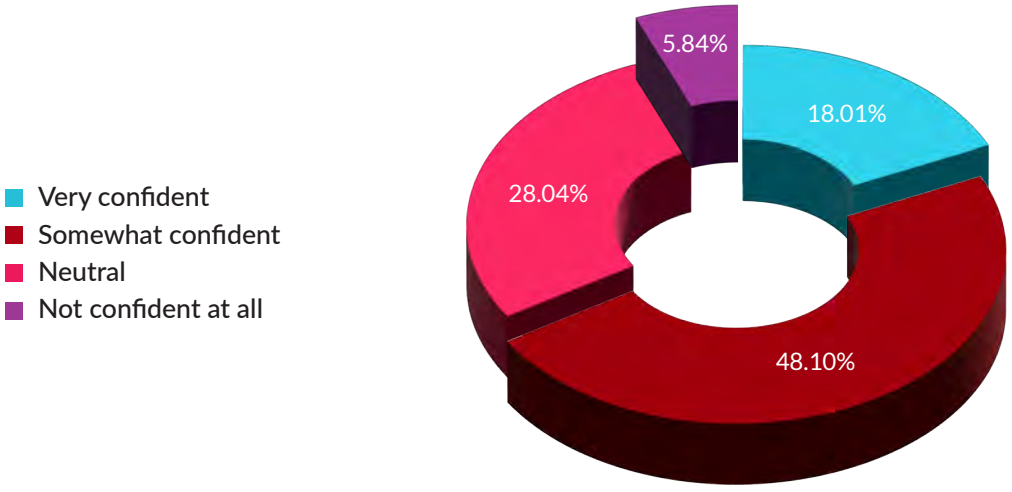
**66%** predict that AI will help in anomaly detection.

**51%** believe that malware detection can be improved with AI/ML.



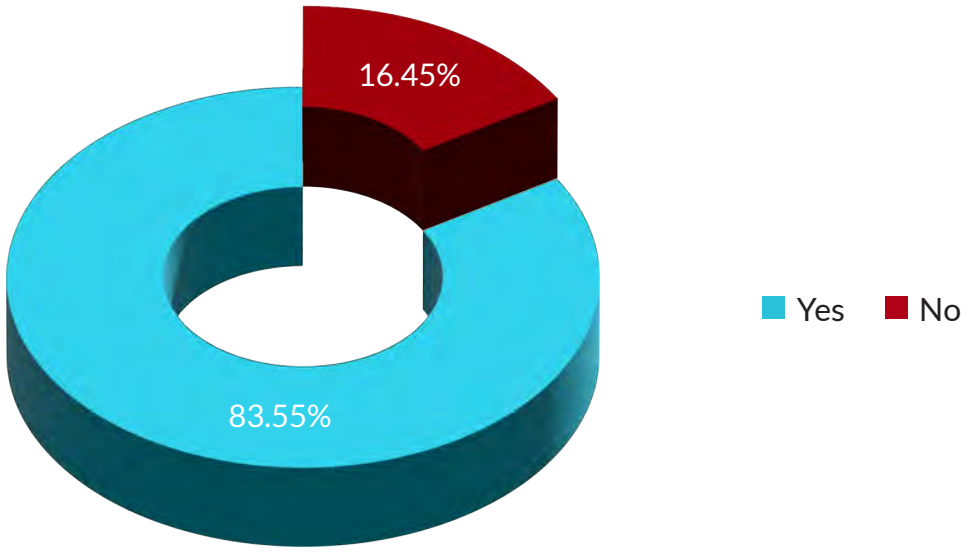

## 6 Confidence in AI's Defense: a Surprising 6% Remain Skeptical

Regarding the use and application of AI in defending against AI-powered cyber attacks, 18% of the respondents are confident that it could help an organization. In comparison, 49% feel somewhat confident, and 27% are neutral. A mere 6% express doubts about AI's capability to defend against AI-generated cyber attacks.



# 7 A Shift in the Winds: 83% Note Tangible Alterations in Attack Methodologies Amidst AI Revolution

As AI advances, 83% of participants believe there will be a rapid evolution of attacks with AI. Organizations must stay vigilant with today's threats and trends in AI and have the right cybersecurity professionals in the right roles. It is essential to ensure that cyber professionals stay on top of their certifications, continue growing their skill sets, and build on their education and network. The more collaboration and training opportunities there are, the more organizations can prepare security professionals to counteract the sophisticated threats that AI and hackers develop.



### How AI Report Findings Can Be Helpful for a Cybersecurity Professional

The threat report indicates that AI's future can benefit many organizations by helping them defend against internal and external threats. The use of AI can assist IT and security professionals with threat detection. Cyber professionals handle and process significant data between monitoring and processing. AI can assist with filtering and evaluating what is normal and what is an anomaly.

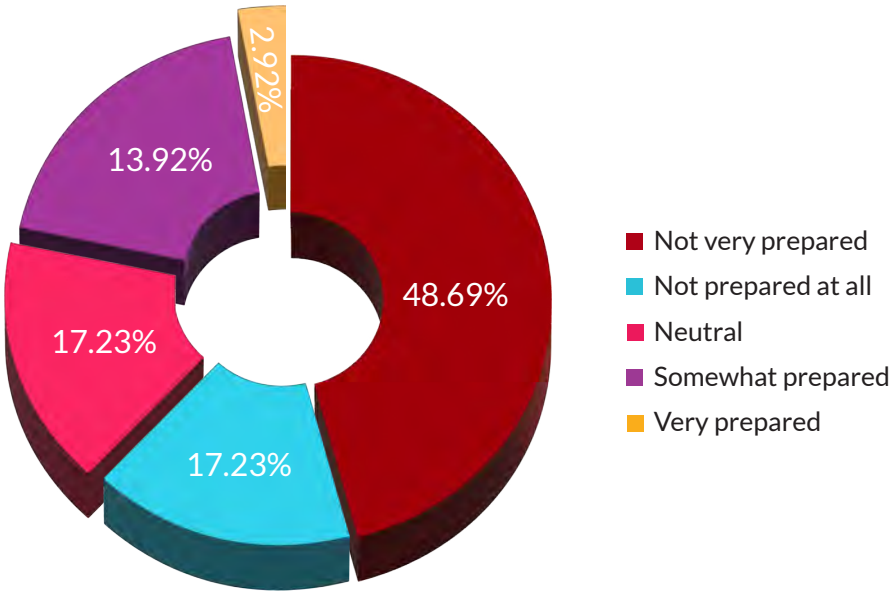
AI can help the cyber workforce to automate, monitor, and analyze unusual behaviors and patterns within a network. Automating redundant, time-consuming tasks can work like a force multiplier when scanning data, using pattern recognition, or identifying IoCs the human eye can miss in larger datasets. In addition to automating tasks with AI, machine learning is also important. AI's ability to learn from previous attacks on a network can be advantageous to learning and identifying new patterns quickly and proficiently. AI can assist security professionals with developing new countermeasures to attacks. AI will only increase, yet no one knows how it will impact companies, our military and how our adversaries will use it against us in the future.

## Threats & Vulnerabilities

Although the use of AI has the potential to provide many great benefits, there are concerns about the capabilities of using AI. Rapid technological advances are making it difficult for security professionals to keep up. The need for more skilled cybersecurity professionals adds to the threats and vulnerabilities. At the same time, educational institutions need help teaching and developing current cybersecurity curricula to prepare students for the workforce.

# 8 AI Readiness: 66% Admit Being ill-Prepared for AI Cyber Onslaughts

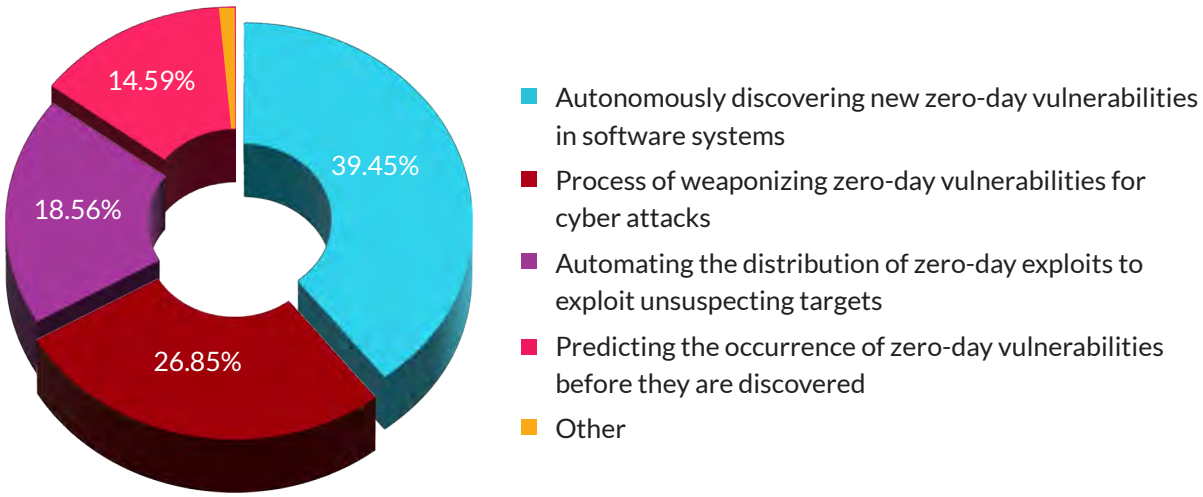
One of the challenges is for students to take theory and apply practical, real-world knowledge and skillsets. Trying to do more with fewer people is creating burnout among security professionals. Addressing a lack of training and education on the job creates potential vulnerabilities for a company, as it takes skilled professionals from their roles to train others. When there are not enough people in an organization to learn and apply very specialized skill sets, organizations often struggle with having IT professionals step into the roles of security professionals without the proper training or credentials, which is not feasible when they are trying to protect critical infrastructures.




While the need for skilled and trained cyber professionals is on the rise, organizations must also face risks from specific targeting, lack of trust from the public, and the manipulation of biased data that can influence national security. Additional risk elements include threats that AI can pose to our democracy for elections, the healthcare system, and public safety concerns. AI can impact social media through psychological exploitations of society while increasing data breaches and identity theft through creating and manipulating deepfake videos.[12] Research indicates that with the prevalence of AI, the following attack vectors will become the hardest to defend.

## 9 Zeroing in on Zero-Day: 68% Stated that These Exploits are Utmost Challenges

Zero-day exploits are unknown vulnerabilities for hardware or software. Networks that are not protected allow hackers to attack before the vendor has a fix for the exploit. 39% of the survey participants believe that AI will play a role in developing and deploying zero-day exploits, and 27% state that the AI process of weaponizing zero-day vulnerabilities for cyber attacks is a threat.




## 10 AI's Social Subterfuge: 60% Predict that AI-Enhanced Social Engineering Will Pose a Significant Challenge

Today, hackers and cybercriminals can collect a great deal of information from various sources and manipulate this data to target specific individuals or organizations, known as spear phishing. AI-enhanced social engineering will allow attackers to create more sophisticated, automated scams.

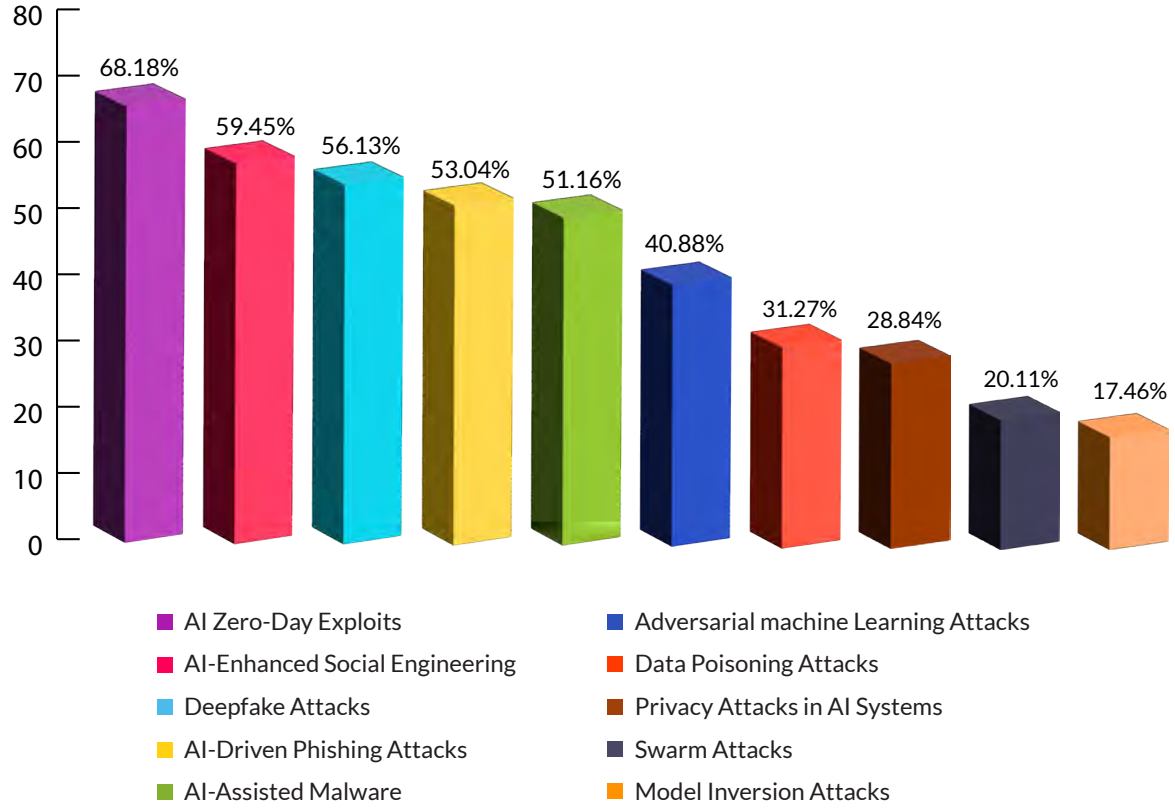
**Respondents indicate that 56% of deepfake attacks will become more prevalent and harder to defend.**

## Top 3 attack vectors that will become the hardest to defend against:

**AI Zero-Day Exploits**

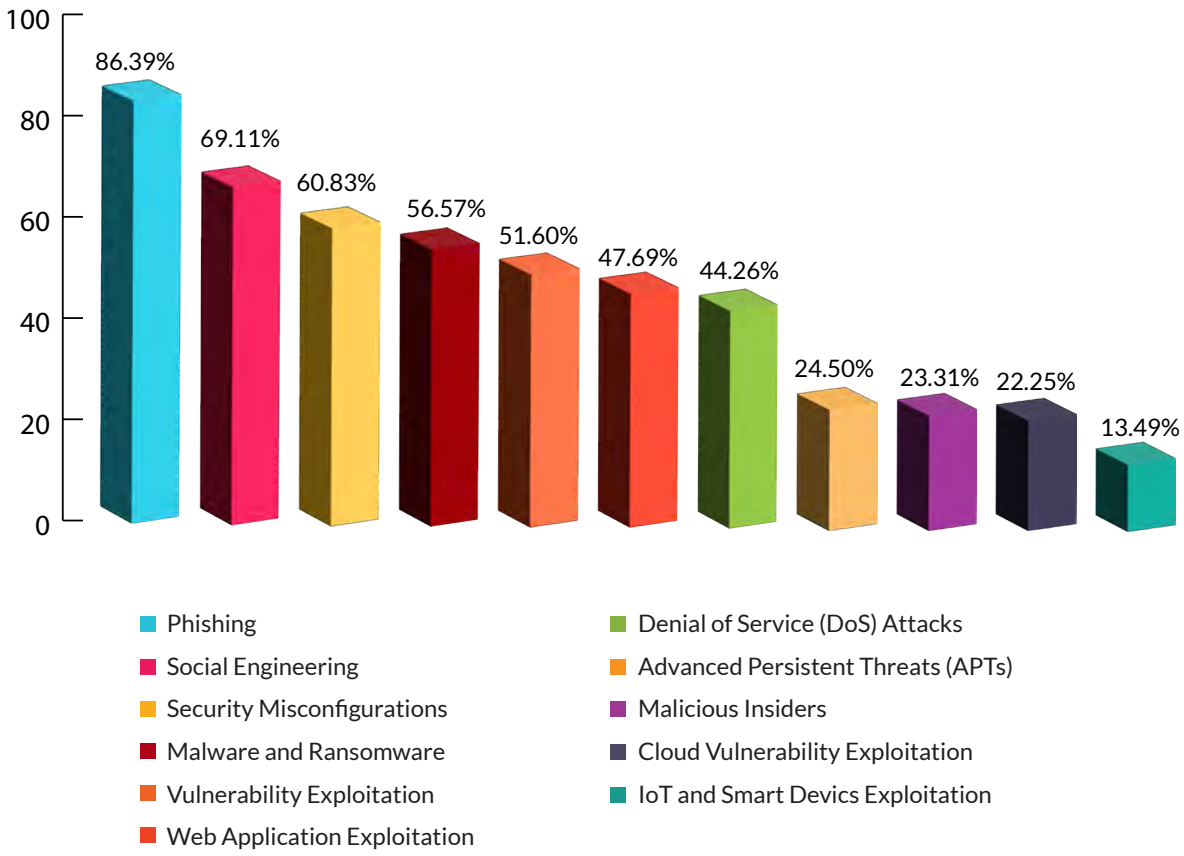
**AI Enhanced Social Engineering**

**Deepfake Attacks**




# 11 The Phishing Epidemic: 86% Report Being Victims

Participants from the study reveal that many organizations experienced various attack vectors in the last 12 months. They include phishing at 86%, malware and ransomware at 56%, social engineering at 69%, malicious insiders at 23%, and security misconfigurations at 61%. Phishing remains the most common attack vector companies encounter.




## 12 Configuring Security: Over 50% Point to Misconfiguration Issues.

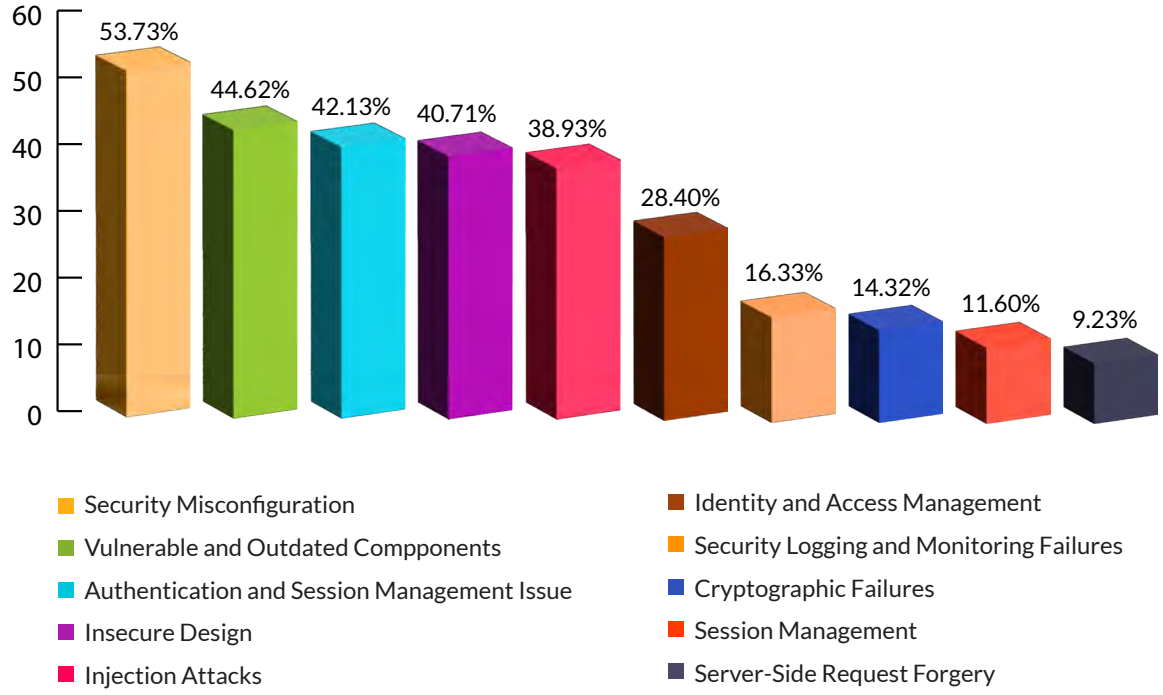
In addition to the top five attack vectors, 56% of the surveyed security professionals cited security misconfigurations among the most severe security vulnerabilities. In contrast, 45% answered vulnerable and outdated components, and 42% cited authentication and session management issues.

### Top 3 application security vulnerabilities:

**Security Misconfiguration**

**Vulnerable and Outdated Components**

**Authentication and Session Management Issues**



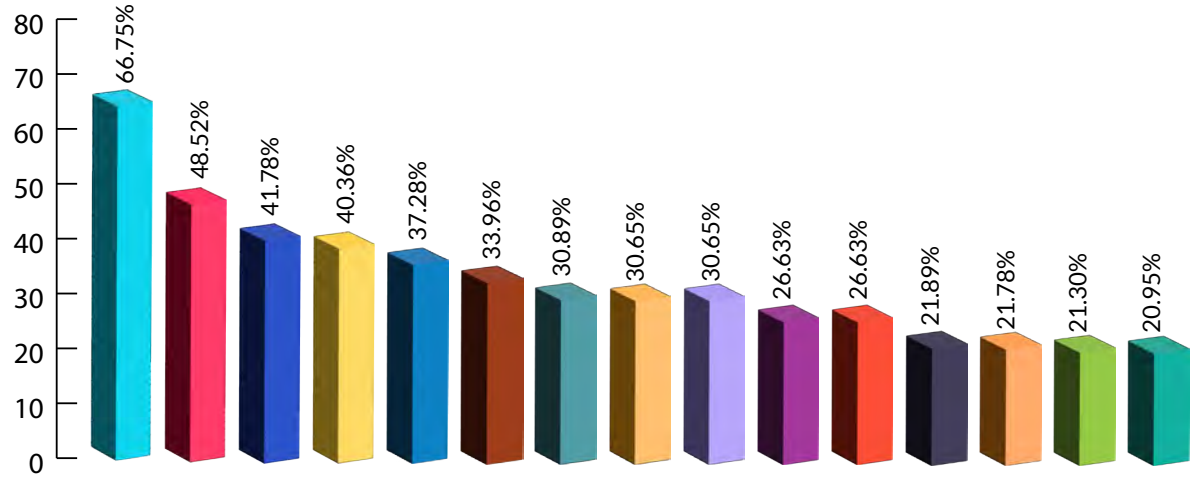

## How Threat and Vulnerabilities Report Findings Are Helpful for a Cybersecurity Professional

Attackers will continue to find ways to manipulate systems and networks for personal benefits, financial gain, or political agendas. As attack tools become more accessible online and AI continues to evolve, many attack vectors will increase, creating more work and security issues and leaving organizations more susceptible to attacks. Ensuring that employees are adequately trained and screened, ensuring a minimum level of access to resources, and ensuring that professionals have the proper skill sets and are certified is a start. Developing a disaster and recovery plan and being vigilant of insider threats is critical to avoid becoming a target.

Malicious insiders are a common threat to organizations, whether big or small. According to the Cybersecurity and Infrastructure Security Agency (CISA), an insider threat is "someone who will use their authorized access, intentionally or unintentionally, to harm the department's mission, resources, personnel, facilities, information, equipment, networks, or systems. Insider threats manifest in various ways: violence, espionage, sabotage, theft, and cyber acts." [13] Some organizations can become complacent with employees, but they must remember that employees can be the biggest threat to the company if they have access to anything or anyone. Being vigilant, engaging with employees, and providing periodic training on company policies and damaging attacks are essential to deter insider threats.

# 13 The Human Element: 67% Warn of a Shortage of Skilled Cloud Security Personnel

One way to resolve some of the major concerns and issues is to hire employees with updated certifications like the Certified Ethical Hacker (C|EH) and Certified Penetration Testing Professional (C|PENT). These two certifications provide the necessary skills to think and plan like a hacker. These certifications also prepare professionals with the latest tools, attack methodologies, and concepts that hackers use to target organizations all around the worldworldwide. Professionals who handle incident reporting will benefit from the Certified Incident Handler (E|CIH), Certified Threat Intelligence (C|TIA), and Certified SOC Analyst (C|SA). Many other industry certifications help build the foundation of security knowledge and concepts while providing professionals with a proactive cybersecurity approach that enables organizations to identify gaps and issues proactively. EC-Council provides several options for those who want to focus on a Cybersecurity Career Track.




- Lack of Trained People
- Inadequate Security Expertise
- Lack of Visibility and Control
- Misconfiguration and In adequate Change Control
- Lack of Cloud Security Architecture and Strategy
- Insecure Interfaces and APIs
- Unsecure Third-Party Resources
- Data Breaches and Leaks
- Poor DevSecOps Practices
- Shared Responsibility Model Confusion
- Insufficient Identity and Access Management
- Rapid Pace of Change
- Compliance Challenges
- Insider Threats
- Shadow IT

# 14 Vigilance in Traffic: 73% Emphasize the Importance of Monitoring Unusual Network Patterns

## Top 5 (IoCs) that can help organizations detect cyber threats:

**Unusual Network Traffic Patterns**


**Outbound Connections to Malicious IP Addresses or Domains**

**Anomalous User Behavior**

**Unauthorized Access Attempts**

**Suspicious Files or Processes**

When detecting cyber threats, 73% of the surveyed professionals state that knowing unusual network traffic patterns in an organization is essential. 67% of the participants report that paying attention to outbound connections to malicious IP addresses or domains is vital to filtering networks that can deny access to those sites. Nothing is more frustrating and concerning than when network traffic patterns fluctuate, creating latency issues for users and high resource utilization on data servers, websites, and overall network traffic. Creating alerts for critical network resources when high usage occurs is a good start to help detect unusual patterns. Observing and restricting (blacklist IPs) where users go outbound on the network and determining who is potentially accessing the network is equally important.

Limiting the risk of network resource access and monitoring inbound and outbound traffic can help detect and reduce potential insider threats. Limiting privilege and access based on the "need to know" principle is crucial. Every employee in the organization will not need access to all resources within the company. Each person has a specific role, and those who work in critical functions with significant data access must have senior-person oversight with two-person integrity. The supervisor or senior person who has been with the company a long time and properly vetted would typically oversee and manage the access to resources.

Including proper training and implementing policies, guidelines, and legal documentation are processes that must be evaluated periodically. Employees must be aware of what is authorized and what is unauthorized access. Background checks, financial checks, education and certification verifications, non-disclosure agreements (NDA), and

non-compete clauses hold employees accountable for not sharing proprietary information when they go to another company.

67% of the respondents state that other indicators of compromise include unauthorized access attempts. IoCs are known as attacks that have already taken place within an organization. At the same time, 60% believe that anomalous user behavior familiarization is essential, while 57% of the participants believe blocking suspicious files or processes is essential. When IT and security administrators control their networks, they can establish baselines and profiling that enable professionals to understand their networks' user behavior and look for deviations.

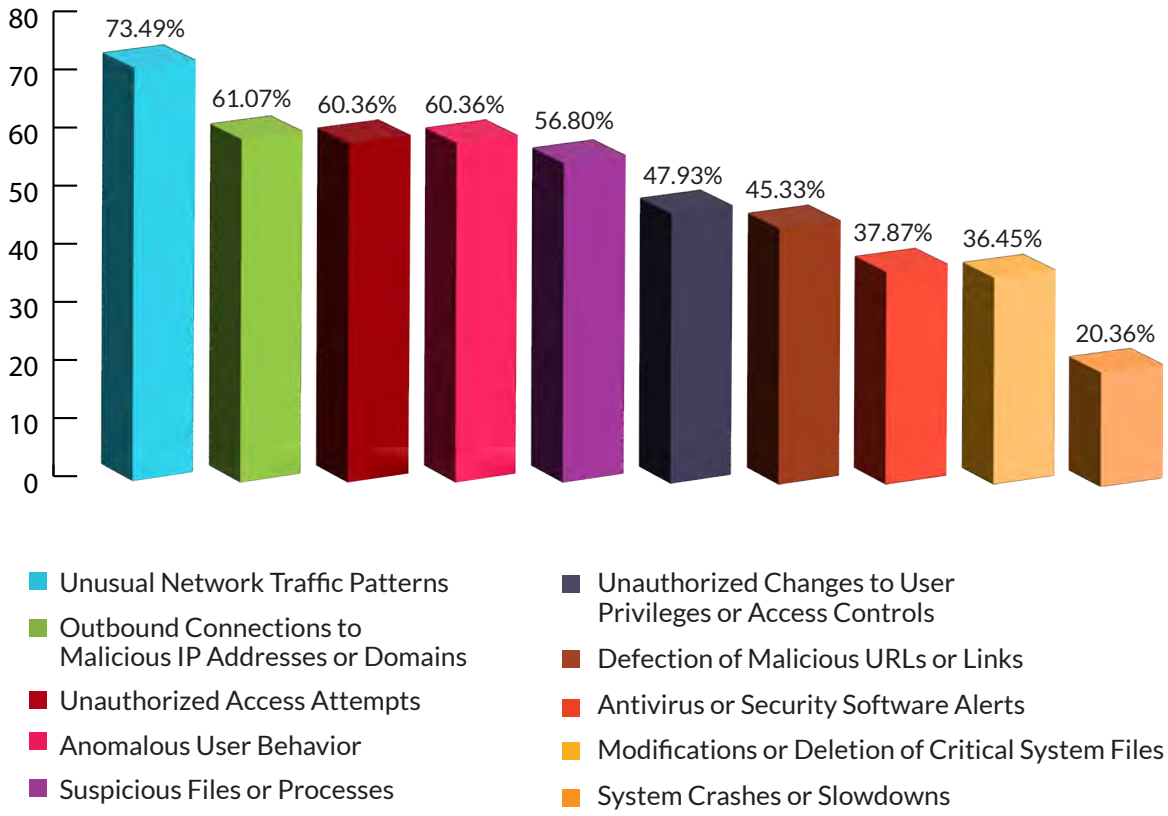
Training professionals on responding to indicators of attacks (IOA) is essential to ensuring that organizations are not merely reactive to indicators of compromise. If cyber analysts are aware and trained on tools and how to respond in the event of an attack, they can contain the incident before any form of data compromise and aid in developing plans for future threats. Being proactive provides practical strategies for stopping the threats or attacks while they occur and responding to attacks before damage can be done to a network.

Strategies that can assist IOA include monitoring traffic coming in and out of the network. TCP (Transmission Control Protocols) and UDP (User Data Protocols) are communication standards that send and receive data over a network checking for open ports that are not required or used and closing them when not in use is one way to help with IOC and IOA. With more than 100,000 ports, knowing which ports are necessary for business operations and closing the ports not in use can help deter attackers. Keeping ports open that are not in use makes it easy for attackers to transmit any form of malware.

Performing network scans on internal hosts can be one method to determine if there is an attacker on the network. Establishing allowlists and blocklists for client network access is essential to preventing attackers from gaining access from one target to another. Policies for users to limit unnecessary website access can also help deter attacks. Analysts need to block access if an unusual IP or user account is accessing resources before the attacker grants additional access.

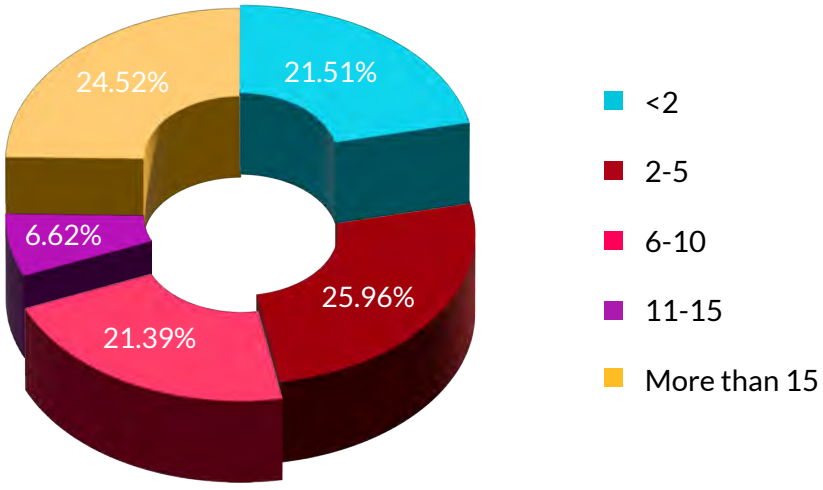
Password policy changes and user login limitations are also beneficial. Some administrators on a network may sometimes change their passwords, while others use the same password multiple times. Using the same password repetitiously can lead to potential compromise in a network. [14] If someone is logged into a system during unusual periods, not during regular business hours, it can indicate an attack is happening and should be disabled.

If the user is logged into multiple systems, it can also indicate that someone with compromised credentials has unauthorized access to the network. Applying IOC and IOA can help cyber professionals develop more robust and secure baselines for network devices, which can help with unauthorized access and observing unusual behaviors and vulnerabilities.



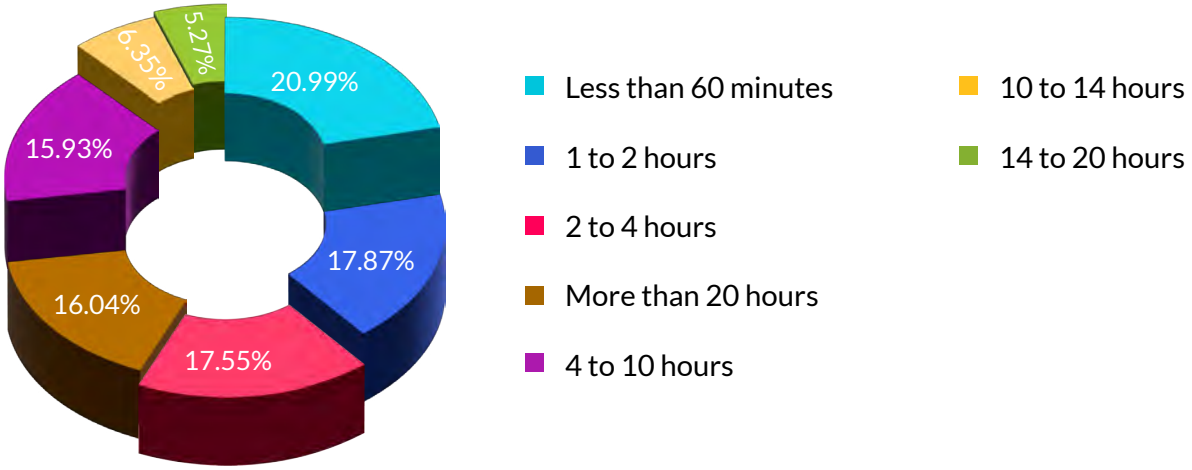

## 15 Visibility Concerns: Nearly 50% Detect Less Than 5 Vulnerabilities During a 30-Day Span

On average, 22% of the surveyed professionals detect less than 2 vulnerabilities during a 30-day period, while 26% of the respondents detect between 2 to 5 vulnerabilities during a 30-day period.



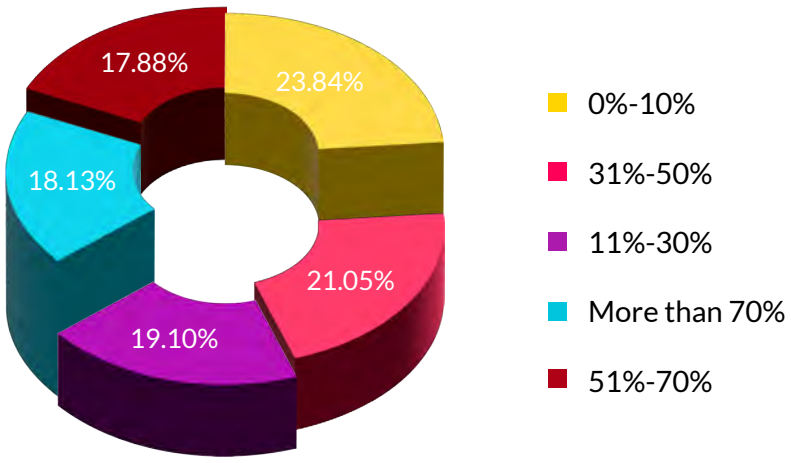
## 16 Response Times: 62% Claimed Taking More than 2 Hours to Respond to an Issue

Once a threat is detected, response times are critical. The longer a breach is left unaddressed, the more opportunity hackers will have to damage the network or target, exfiltrate sensitive information, and set up contingency plans for the organization's countermeasures. Data shows that many organizations need to develop and improve response times when a threat is detected.




## 17 Resolution Time: Only 10% of Attacks Were Resolved in Under 60 Minutes

In a recent survey, 819 professionals were asked about the number of attacks they encountered in the last 12 months, and 24% stated that 0-10% of attacks were resolved in under 60 minutes by the host organization.



# 18 Cloud Attack Dynamics: 67% Confirmed That the Exploitation of Weak or Stolen Credentials Is a Top Cloud Attack Tactic

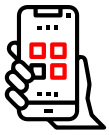
**Top 5 tactics, techniques, and procedures (TTPs) commonly employed in cloud-based attacks**

**Exploitation of Weak or Stolen Credentials**

**Misconfigured Cloud Storage Breaches**

**Account Hijacking and Unauthorized Access**

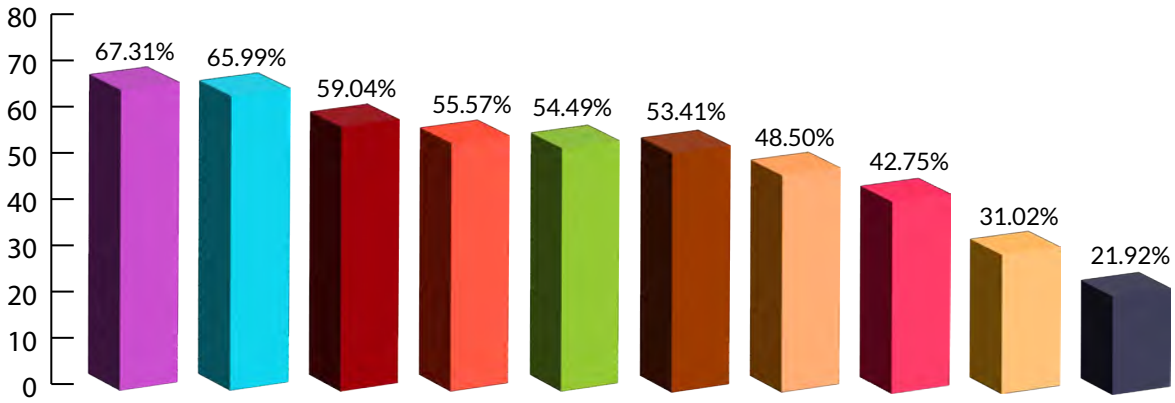

**API Abuse and Exploitation**



**Insecure Application Deployments in the Cloud**

System misconfigurations constitute a significant risk for organizations. Many companies purchase software intending to use it but need to correctly configure or thoroughly test it in a sandbox environment. This leaves networks and resources vulnerable to risks and attacks. [14] The misconfiguration of software can lead to a false sense of security, costing organizations millions of dollars and impacting their reputations. Over the last five years, cloud computing has been the most popular trend in software management. Companies pay a lot for cloud technologies but only sometimes fully understand the security implications. Companies seek cloud-based technologies to remediate the risk while passing the risk to third-party cloud technologies.

Participants were asked about the top five tactics, techniques, and procedures commonly employed in cloud-based attacks. These respondents identify the exploitation of weak or stolen credentials (67%), misconfigured cloud storage breaches (65%), account hijacking and unauthorized access (59%), and insecure application deployments in the cloud (56%) most often.




- Exploitation of Weak or Stolen Credentials
- Misconfigured Cloud Storage Breaches
- Account Hijacking and Unauthorized Access
- Insecure Application Deployments in the Cloud
- API Abuse and Exploitation
- Cloud Phising and Social Engineering Attacks
- Unauthorized Data Exfiltration from Cloud
- Dos attacks on cloud services
- VM Hopping and Lateral Movement in Cloud Networks
- Malicious insider Activities in the Cloud

## 19 Layered Defense: 80% Employ Multi-Factor Authentication to Combat Top 5 Cloud Threat Tactics and Procedures (TTPs )

**Top 5 countermeasures employed to mitigate the risks associated with the top 5 cloud TTPs**

**Multi-Factor Authentication (MFA)**

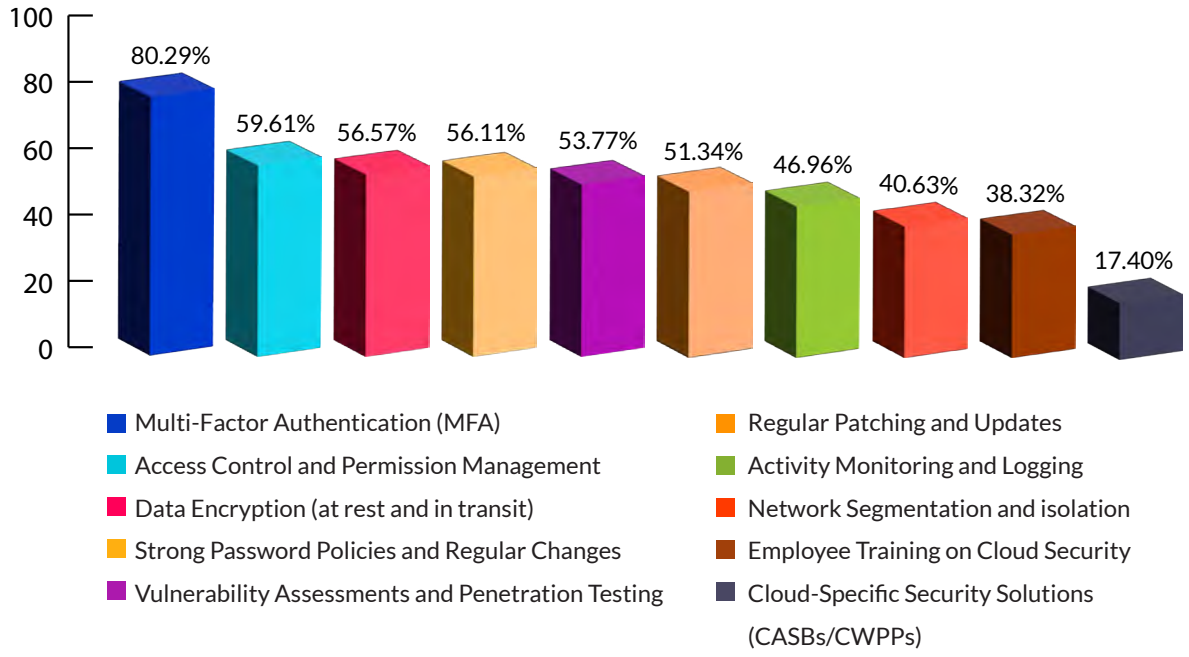
**Access Control and Permission Management**

**Data Encryption (at rest and in transit)**

**Strong Password Policies and Regular Changes**

**Vulnerability Assessments and Penetration Testing**

Organizations worldwide have adopted some form of cloud-based technology to help alleviate the workload and shortage of IT and security professionals. Cloud-based technologies are a great tool to save money and resources, but security needs to be at the forefront of using cloud technologies. IT and security professionals were asked about the top 5 countermeasures or security practices regularly employed to mitigate the risks associated with cloud TTPs. 80% respond that multi-factor authentication (MFA) is one way, while 60% state that access control and permission management are another. Data encryption (56%) strong password policies, and regular account changes (55%) are important to safeguarding cloud technologies.



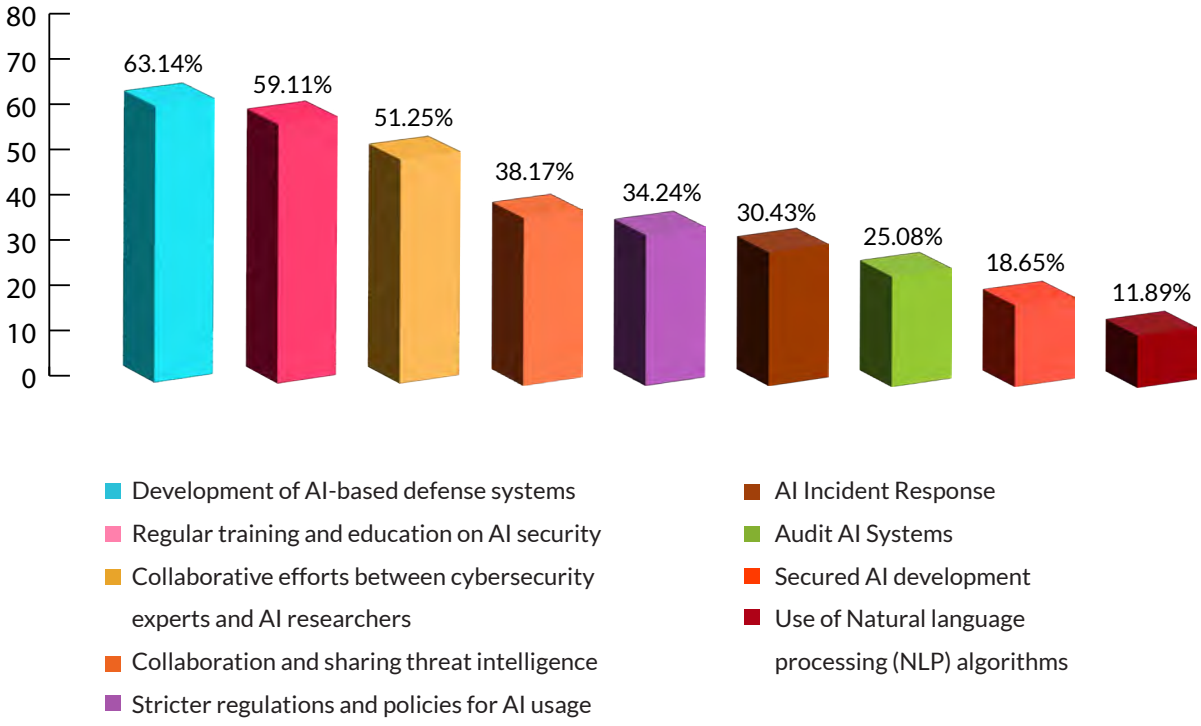

## 20 AI's Defensive Potential: Over 60% Believe AI-Based Training and Development are Key to Risk Mitigation

Participants were asked what measures they believe should be taken to mitigate the risks of AI in cyber attacks.

**Development of AI-based defense systems (63% ranked it as no.1)**

**Regular training and education on AI securitys (according to 59%)**

**Collaborative efforts between cybersecurity experts and AI researchers (51%)**




The development of AI-based defense systems can be advantageous but time-consuming and expensive. Due to the cyber workforce shortage and heavy demands on IT and security professionals, allocating time and effort to create AI-based defense systems can take time. One option is outsourcing through major IT companies specializing in creating automated systems through AI. According to IBM, AI systems can help with life cycle management and machine learning implementation. These solution providers can help build trustworthy AI while increasing efficiency through unifying tools, processes, and people[15].

Regular training and education on AI security is essential. AI is still a reasonably new technology. Although AI has been around for about 60 years, society has shifted a focus toward AI for many companies and educational institutions. However, only some professionals are properly trained or educated in AI. Organizations that adopt AI/ML must be familiar with the capabilities, have a thought-out plan for using it, and consider the implications of using AI. Companies must ensure all users have the proper training through various courses before using AI.

Collaborative efforts between cybersecurity experts and AI researchers are essential in building knowledge that will contribute to AI-driven detection and mitigation strategies.

# 21 Bypassing the Barricades: Over 70% Identify Social Engineering and Zero Day Exploits as Top Threat Vectors

Attending conferences, AI and security forums, training, and collaboration between companies and agencies help researchers stay ahead of hackers and threats that emerge through AI. Additional concerns for collaboration and research about AI are standard techniques used by threat actors to bypass existing security measures, including the following:

**Advanced Social Engineering**

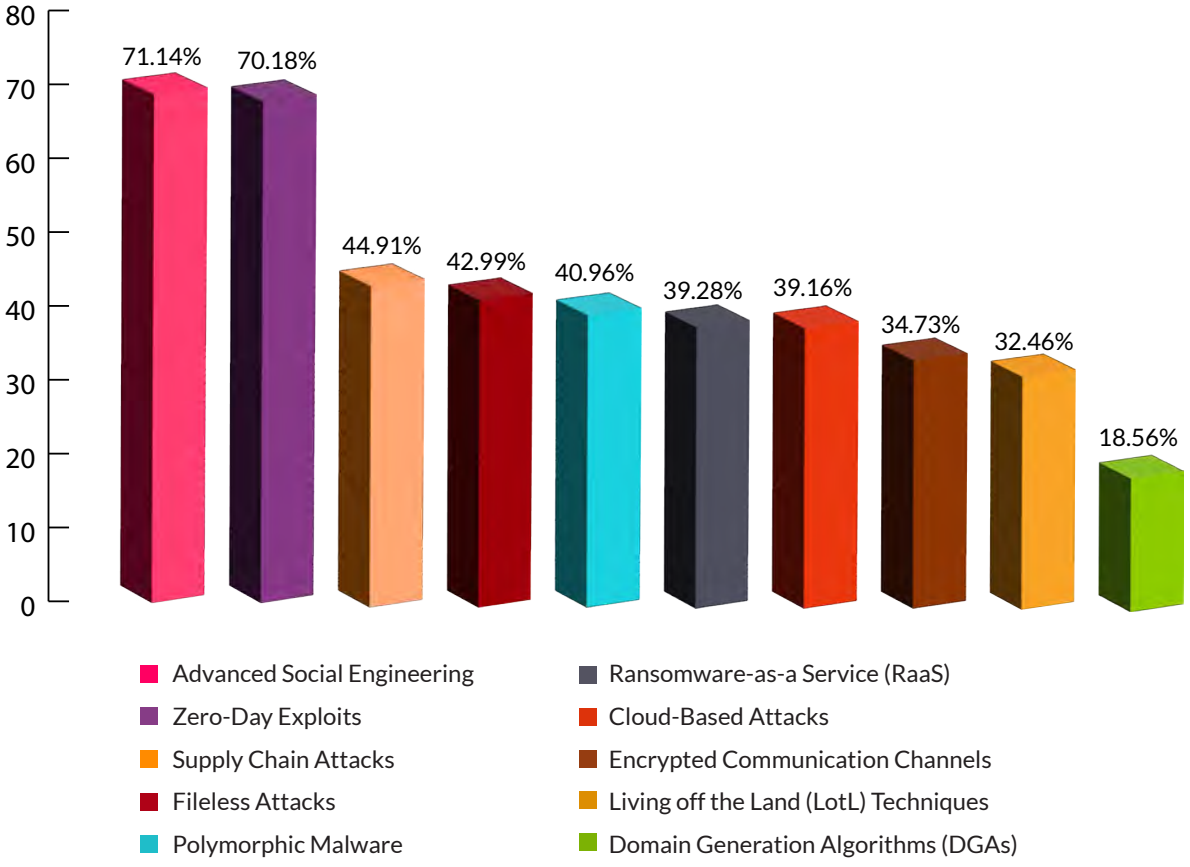
71%

**Zero-Day Exploits**

70%

**Supply Chain Attacks**

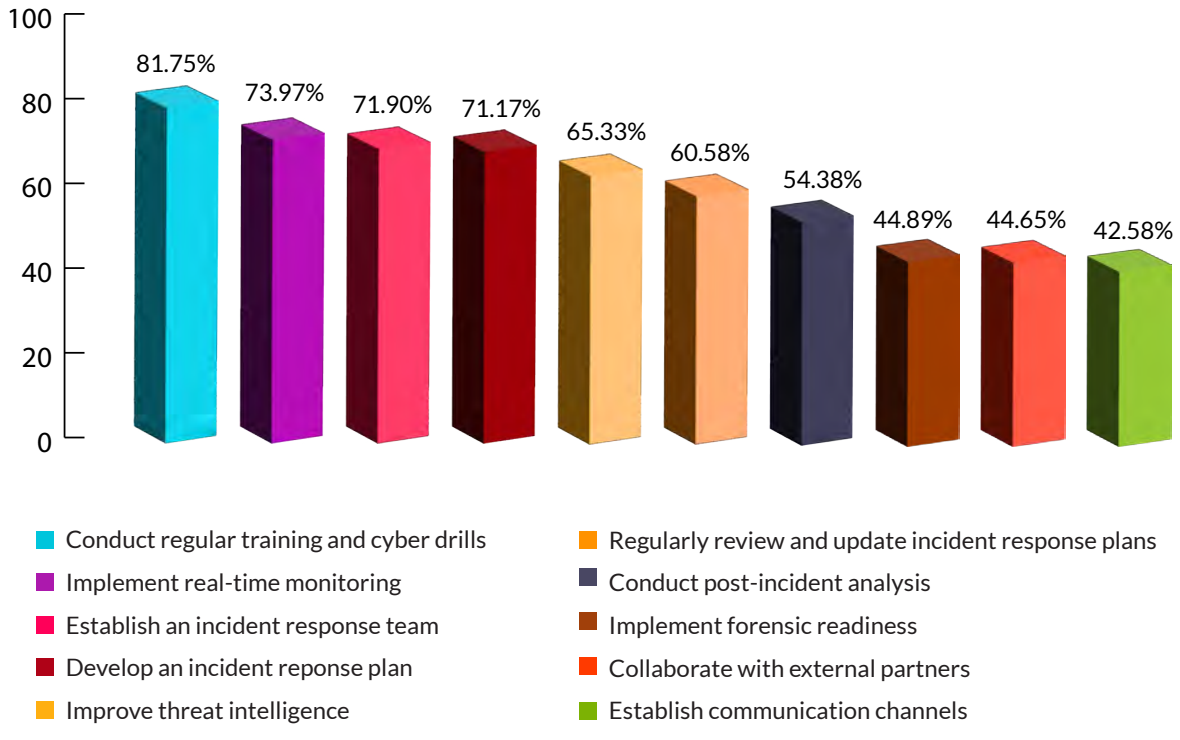
45%



# 22 Education's Edge: 82% Champion Regular Training for Incident Response

The mitigation process requires careful planning and evaluation of the threats and incidents in an organization. Participants were asked what the best ways are to enhance incident response capabilities to minimize the impact of a successful attack. 82% state that regular training and cyber drills are beneficial. Many threats and attacks typically occur because of employees. Some attacks are intentional, while others are due to a lack of awareness and training.

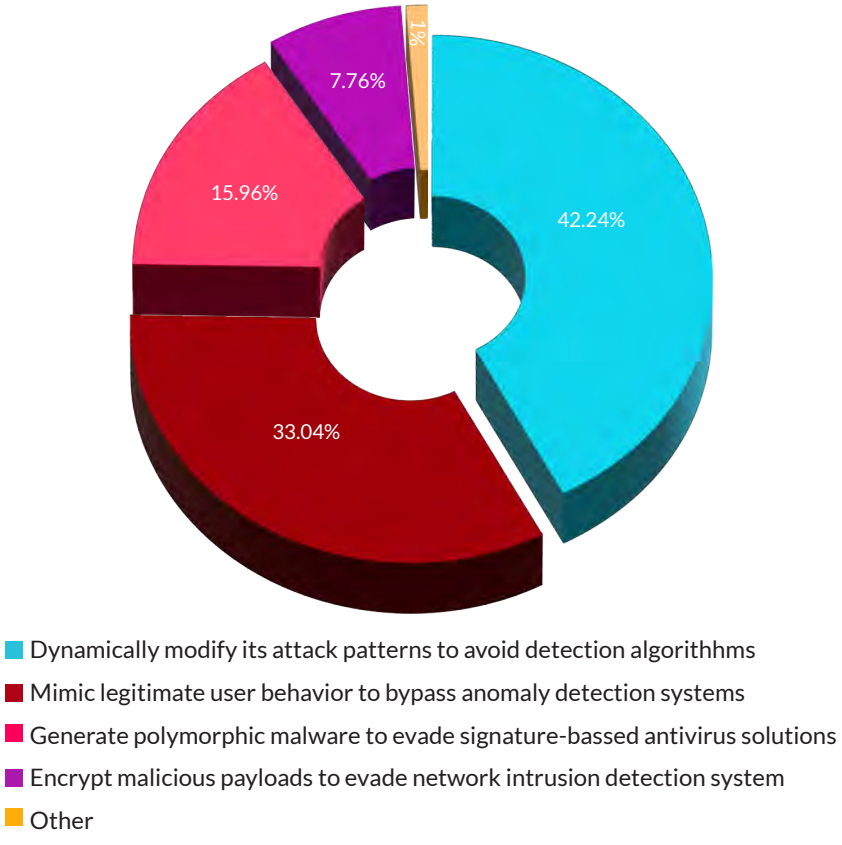
Real-time monitoring (74%) is the second-best approach to minimizing the impact of a successful attack. 72% of the participants note establishing an incident response team and plan is essential. Applying different methods and multiple techniques in an organization can help make everyone aware of threats and hold employees accountable for their actions. Testing the incident response plans will ensure everyone has their role and expectations for each task. The objective is to be proactive and not reactive. If an attack happens, organizations should execute their incident response plan and document the entire process to ensure organization learning and memory builds. This documentation and maturity strengthen IH&R processes and prevent future attacks.



# 23 Evolving Adversaries: 42% Predict AI's Adaptability in Attack Patterns to Avoid Detection Algorithms

To evade detection by traditional security systems, 42% of IT and security professionals recommend that organizations use AI to modify their attack patterns to avoid detection algorithms dynamically. 33% of the respondents state that organizations mimic legitimate user behavior to bypass anomaly detection systems, and 16% suggest that organizations generate polymorphic malware to evade signature-based antivirus solutions.

**How can AI be used to evade detection by traditional security systems?**



# 24 Summary: The Latest Best Practices by Ethical Hackers

Ethical hackers' recent best practices are ensuring they can handle threats. Regular training and cyber drills with real-time and consistent monitoring and establishing incident response teams and plans while improving threat intelligence are the top best practices to help deter attacks. Over 60% of participants feel that regular review and update of incident response plans is essential, and 54% state that performing post-incident analysis will help with behavior analysis and a better understanding of future attacks.

No organization is completely immune to attacks and threats. Companies must provide consistent cybersecurity training and awareness to all employees. The training will teach them about the latest phishing scams and social engineering techniques. 45% state that collaboration with external partners helps minimize the impact of a successful attack, while 42% believe the same about open communication channels.

Limiting access to resources, applying worker access control, applying the "need-to-know" principle for job roles, and applying firewalls, DMZ, honeypots, and load balancers are helpful. Implementing security policies for access, setting limited time constraints of when personnel can log into the network resources (only during business hours), enforcing vacation access policies, and periodic job-rotation policies linked with administrative security controls are helpful tactics. Ensuring there is a two-person integrity in data management, applying password change policies, network monitoring tools, and host-based monitoring can help security professionals analyze unusual activity in a network. In addition to the application of secure software and hardware, ongoing cybersecurity training and best practices, updated company policies, user network license agreements, and limited remote abilities using virtual private network (VPN) connections for mobile personnel are simple protective measures and best practices.

# 25 Conclusion

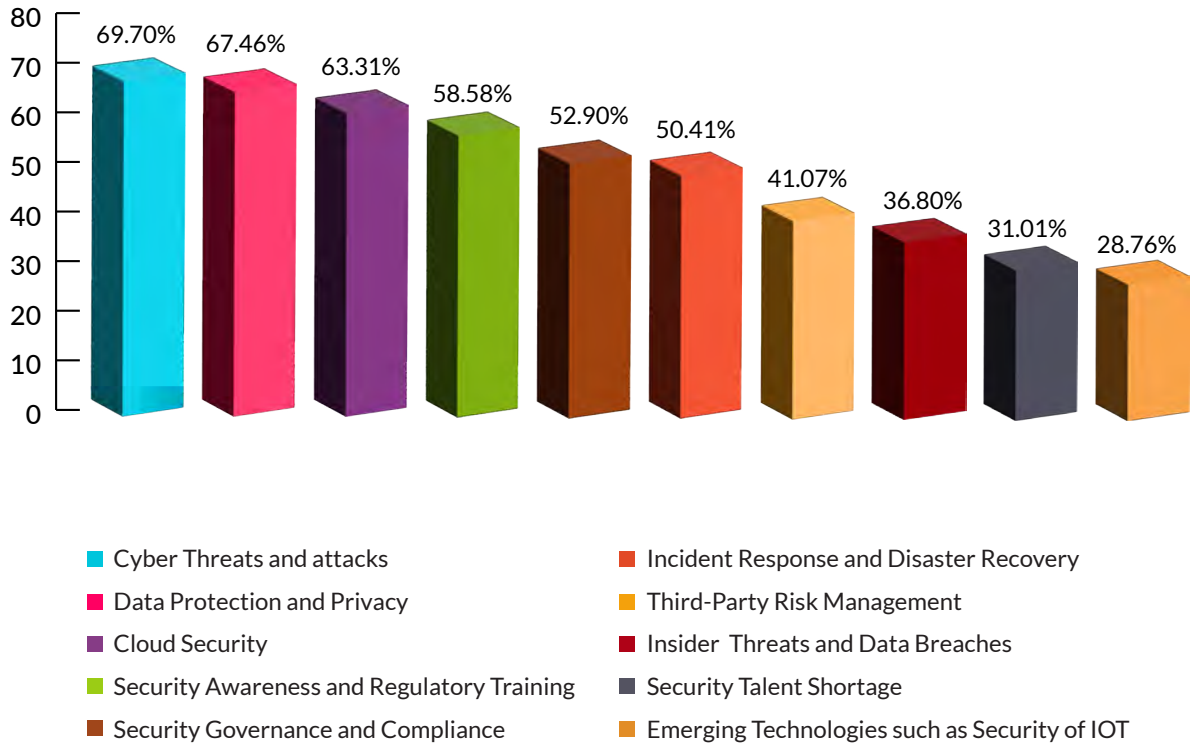
The EC-Council Threat Report for 2024 concludes that the top five attack vectors of phishing, malware and ransomware, social engineering, malicious insiders, and security misconfigurations will be an ongoing issue and concern. These attack vectors will continue to evolve as AI becomes more prevalent. The adoption and use of AI and ML will continue to revolutionize the field of cybersecurity and how organizations detect, respond to, and prevent attacks. Staying on top of the threats and having skilled professionals who understand and think like a hacker while performing penetration tests within their organizations is a start. Organizations need to not only focus on their adversaries but also be aware of attacks that come from insider threats.

Internal threats are a significant concern for the cyber threat landscape. A person inside knows more about the company and has direct access to the resources compared to those external threats. According to the Office of the Director of National Intelligence (ODNI), "Malicious insiders can inflict incalculable damage." [16] Lord states, "Over the past century, a trusted insider with ulterior motives perpetrated the most damaging US counterintelligence failures." [17] Building a solid cyber workforce is essential to ensure organizations meet the demands of attacks, becoming more sophisticated to detect and defend. Recruiting and maintaining high-performing cyber professionals amidst the cybersecurity talent gap will remain an ongoing challenge, with over 3.4 million roles that need to be filled. [18] A recent CSIS survey of IT decision-makers across eight countries found that 82 percent of employers report a shortage of cybersecurity skills, and 71 percent believe this talent gap causes direct and measurable damage to their organizations. Not having the right personnel will result in unsecured systems, increased vulnerabilities, software and hardware misconfigurations, and the inability to respond to attacks quickly.[19]

Over 60% of the respondents identify their organizations' leadership plan to address cyber threats, data protection, and cloud security as their top 3 challenges.

The threat report indicates that the top cybersecurity challenges organizational leadership plans to address shortly include the following: cyber threats and attacks at 70%, data protection and privacy at 67%, cloud security at 63%,

and security awareness and regulatory training at 59% of the responses. While organizations know the threat vectors, it takes careful planning and long-term vision to address the potential threats and attacks. Nothing is a one-stop deterrent, but applying a comprehensive approach to every vulnerability will prepare IT and cybersecurity personnel to secure their networks and resources more effectively.




## 26 About Certified Ethical Hacker (C|EH)

EC-Council's Certified Ethical Hacker (C|EH) is the world's leading ethical hacking credential that equips cybersecurity professionals with the knowledge, skills, and abilities to protect organizations against cyber attacks.

Certified Ethical Hackers are trained to follow a rigorous 5-phase approach (1. Reconnaissance, 2. Scanning, 3. Gaining Access, 4. Maintaining Access, 5. Covering Tracks) when lawfully breaking into an organization to identify the weakest links, vulnerabilities, and misconfigurations. This approach is the blueprint of ethical hacking, where a student learns to understand the mindset of a hacker.

The C|EH is the world's only cybersecurity certification program incorporating a unique 4 phase learning framework of "Learn, Certify, Engage, and Compete."

This unique learning framework covers every aspect from training to certification and hones learners' skills by exposing them to ethical hacking engagements in EC-Council's live cyber range environment. Candidates then get to prove their mettle through a series of Global Ethical Hacking Competitions designed to keep their skills up to date years after the certification. One of the most sought-after certifications globally, the C|EH prepares candidates for various lucrative cybersecurity roles with top Fortune 500 Companies and even in government sectors over 18 years.


### Gain Skills

- 5 Days of Training
- 20 Modules
- Over 220 hands-on-labs with compilation flags
- Over 3,500 Hacking Tools
- Learn how to hack multiple operating systems
- (Windows 11, Windows Servers, Linux, Ubuntu, Android)


### Gain Experience

**C|EH Knowledge Exam**

- 125 Multiple-Choice Questions
- 4 Hours
- ANAB 17024 Accredited

**C|EH Practical Exam**

- 6 Hours Practical Exam
- 20 Scenario Based Questions
- Prove Your Skills And Abilities


### Gain Recognition

- Conduct A Real-World Ethical Hacking Assignment
- Apply The 5 Phases
  - Reconnaissance
  - Scanning
  - Gaining Access
  - Maintaining Access
  - Covering Your Tracks


### Gain Respect

- New Challenges Every Month
- 4 Hour Competition
- Compete With Your Peers All over The World
- Hack Your Way to the Top of the leaderboard
- Gain Recognition
- Challenges

# 20 JOB ROLES MAPPED WITH C|EH

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- Information Security Analyst 1
- Security Analyst L1
- Infosec Security Administrator

- Cybersecurity Analyst level 1, level 2, & level 3
- Network Security Engineer
- SOC Security Analyst
- Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant

According to Talent.com, the average annual pay for a Certified Ethical Hacker in the United States is $125,000 annually.

# Acreditations, Recognitions & Endorsements


The national Initiative for Cybersecurity Education (NIC)


American National Standards Institute (ANSI)


Cyber Workforce Qualification Program



National Infocomm Competency Framework (NICF)


MSC


KOMLEK

# 27 The Impact of C|EH on Cybersecurity Careers

"Is the Certified Ethical Hacker (C|EH) worth it?" This is a question that countless aspiring cybersecurity professionals have asked, and we bring you information backed by real data collected from thousands of cybersecurity professionals who have successfully pursued the C|EH. Each has trained for the C|EH and applied the newfound skills acquired through the C|EH certification to their jobs as cyber professionals. These cybersecurity professionals have undertaken a career development journey similar to yours. They are now working in the industry, including many that have successfully gained employment in top government agencies or Fortune 500 companies.

## Key takeaways from C|EH Hall of Fame Report 2023

Here are some highlights of what the surveyed respondents said:

**Over 1 in every 2** professionals received promotions after the C|EH

**97%** stated that the skills acquired in C|EH helped safeguard their organizations.

**97%** found that C|EH labs accurately mimic real-world cyber threats.

**95%** chose the C|EH for career growth.

**93%** said that C|EH skills improved their organizational security.

**92%** reported that the C|EH boosted their self-confidence.

**92%** of hiring managers prefer candidates with C|EH for jobs that require ethical hacking skills.

**88%** considered C|EH the most comprehensive ethical hacking program in the industry.

**85%** credited C|EH with helping them give back to the cybersecurity community.

**80%** started their cybersecurity careers with the C|EH.

To Read the C|EH Hall of Fame Report: Click Here

To learn the real stories of Certified Ethical Hackers and the impact of the C|EH: Click Here

# Why People Love C|EH

**MAURICIO** FERNANDES

CISCO

United States of America
Cisco Systems Architect

*"Skills from the C|EH program have evolved and are valuable."*

**ROY** DAVIS

zoom

United States
Security Engineer

*"Knowledge I gained from C|EH gave me the confidence I needed to step into a role as a security engineer and penetration tester."*

**GIULIO** ASTORI

Microsoft

USA
Cyber Security Architect

*"Helping organization investigating SolarWinds hack, wouldn't have been possible without C|EH."*

**FARZAN** KARIMI

Google

United States
IT Security Manager

*"C|EH was my first confidence booster and helped land me a job on a Red Team in the government sector."*

**KOJO** DONKOR

CISCO

United States of America
Security Architect

*"C|EH Made me an authoritative expert on security discussions with our clients."*

**LAWAN** CANCER II

Morgan Stanley

United States of America
Security Analyst

*"C|EH helped me be able to understand exactly what I was doing once I finally landed a role in the cybersecurity field."*

**JOHN** PACKIARAJ

VISA

United States
Security Architect

*"C|EH has helped me to work on mobile devices and AppSec - Pen testing and reverse engineering."*

**SIDHANT** GUPTA

EY

United States of America
Senior Security Consultant

*"C|EH certification made my CV outstanding compared to my peers. Cybersecurity skillset helped me find a better job profile as a fresher."*

**FELIPE** MUNOZ

ORACLE

United States of America
IT Security Director

*C|EH develops a "think outside the box" approach that you cannot get from other skills.*

# 28 About EC-Council

EC-Council's sole purpose is to build and refine the cybersecurity profession globally. We help individuals, organizations, educators, and governments address global workforce problems by developing and curating world-class cybersecurity education programs and their corresponding certifications. We also provide cybersecurity services to some of the largest businesses globally. Trusted by 7 of the Fortune 10, 47 of the Fortune 100, the Department of Defense, the Intelligence Community, NATO, and over 2,000 of the best universities, colleges, and training companies, our programs have increased through over 140 countries. They have set the bar in cybersecurity education. Best known for the Certified Ethical Hacker programs, we are dedicated to equipping over 230,000 information-age soldiers with the knowledge, skills, and abilities required to fight and win against the black hat adversaries.

EC-Council builds individual and team/organization cyber capabilities through the Certified Ethical Hacker Program, followed by a variety of other cyber programs, including the Certified Secure Computer User, Computer Hacking Forensic Investigator, Certified Security Analyst, Certified Network Defender, Certified SOC Analyst, Certified Threat Intelligence Analyst, Certified Incident Handler, as well as the Certified Chief Information Security Officer. We are an ANAB 17024 accredited organization and have earned recognition by the DoD under Directive 8140/8570 and in the UK by the GCHQ, CREST, and various other authoritative bodies that influence the profession.

Founded in 2001, EC-Council employs over 400 individuals worldwide, with ten global offices in the USA, UK, Malaysia, Singapore, India, and Indonesia. Its US offices are in Albuquerque, NM, and Tampa, FL.

Learn more at www.eccouncil.org

# 29 References:


1. Poremba, S. (2023). The cybersecurity talent shortage: the outlook for 2023. https://www.cybersecuritydive.com/news/cybrsecurity-talent-gap-worker-shortage/639724/

2. Donaldson. A. (2021). Executive order on improving the nation's cybersecurity. https://ordinary-times.com/2021/05/12/president-biden-executive-order-on-cybersecurity-read-it-for-yourself/

3. Strengthening American Cybersecurity Act of 2022 https://www.congress.gov/bill/117th-congress/senate- bill/3600

4. Center for Strategic and International Studies (2023). https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

5. Center for Strategic and International Studies (2023).

6. Council of Europe. History of Artificial Intelligence. (2023). https://www.coe.int/en/web/artificialintelligence/history-of-ai

7. Baker, K. (2023). The rise of AI social engineering scams. https://www.identityiq.com/scams-and-fraud/the-rise-of-ai-social-engineering-scams/#:~:text=Machine%20learning%20algorithms%20enable%20scammers%20to%20create%20highly,and%20manipulate%20social%20media%20platforms%20to%20their%20advantage.

8. Council of Europe. History of Artificial Intelligence. (2023). https://www.coe.int/en/web/artificial-intelligence/history-of-ai

9. Council of Europe. (2023).

10. Smith, G. (2018). The intelligent solution: automation, the skills shortage and cyber-security https://www.sciencedirect.com/science/article/abs/pii/S1361372318300733

11. Smith, G. (2018).

12. Sample, I. (2020). What are deepfakes-and how you can spot them? The Guadian. https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

13. Cybersecurity & Infrastructure Security Agency (n.d). Defining insider threats.

https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

14. Miller, W. (2019). iBeta. Risks of not testing software properly. https://www.ibeta.com/risks-of-not-testing-software-properly/

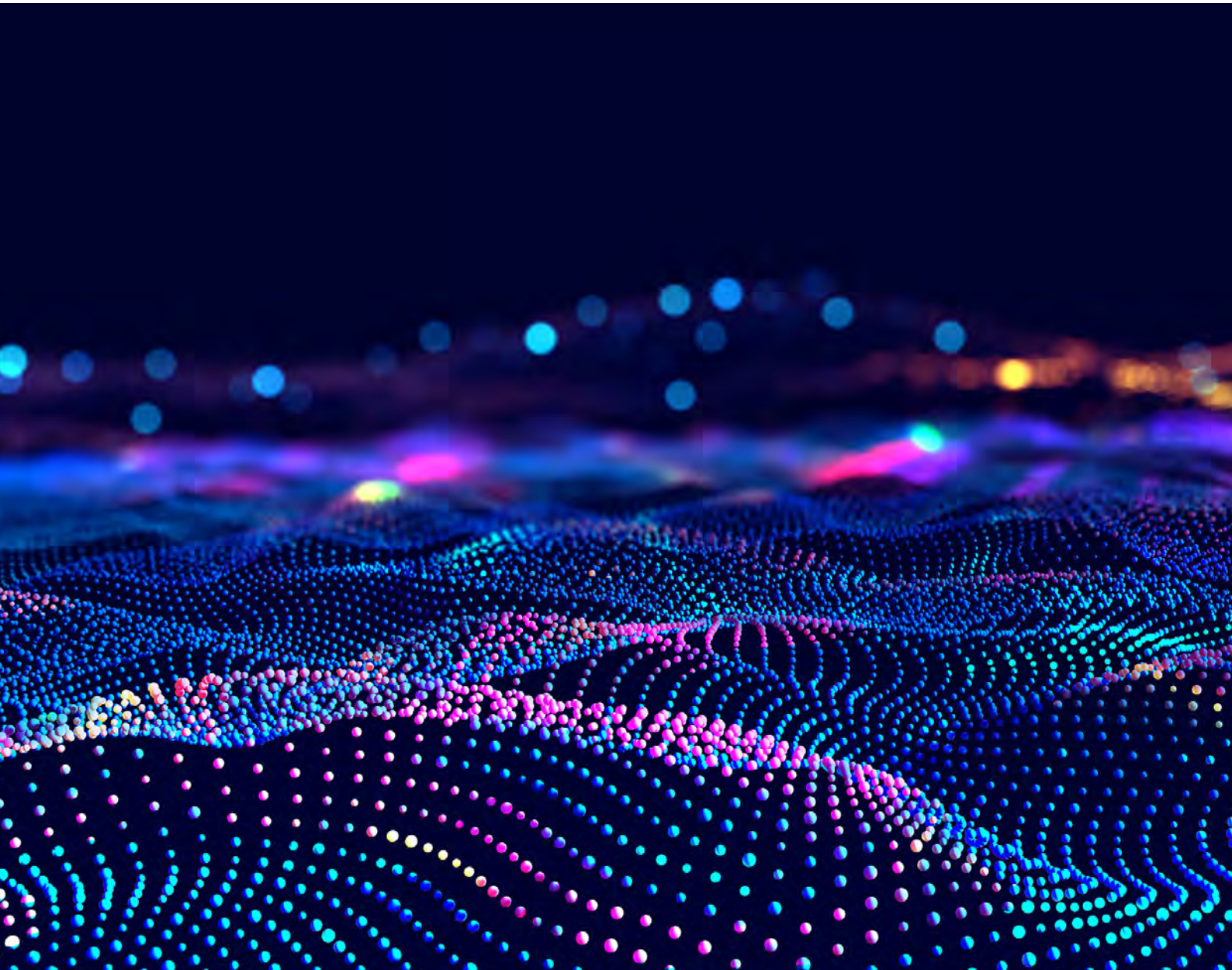
15. IBM. Accelerating AI and Model lifecycle management. https://www.ibm.com/resources/the-data-differentiator/scale-ai

16. Office of Director of National Intelligence (2016). Protect your organization from the inside out: Government best practices. https://www.dni.gov/files/NCSC/documents/products/Govt_Best_Practices_Guide_Insider_Threat.pdf

17. Lord, N. (2023). Digital Guardian. What is an insider threat? An insider threat definition. https://www.digitalguardian.com/blog/what-insider-threat-insider-threat-definition

18. Poremba, S. (2023). The cybersecurity talent shortage: the outlook for 2023. https://www.cybersecuritydive.com/news/cybersecurity-talent-gap-worker-shortage/639724/

19. CSIS, Hacking the Skills Shortage (Santa Clara, CA: McAfee, July 2016), https://www.mcafee.com/enterprise/en-us/assets/reports/ rp-hacking-skills-shortage.pdf.



# Our Special Thanks to the Certified Ethical Hacker Advisory Board Members

## America

**Jeff Sowell**

Cybersecurity Advisor, Solution Security Engineering | Infrastructure Operations | Executive Engagement Ericsson

**Derek A. Smith**

Supervisory Information Technology Specialist - Chief, Internet Service Integration Internal Revenue Service (IRS)

**Brain Curnutt**

Director Microsoft Alliance

**Joe Gray**

Senior OSINT Specialist QOMPLX

**Pete Ryan**

Senior Director, Security Operations & Incident Response at Thomson Reuters Thomson Reuters

**David Kosork**

Senior Director of Application and Product Security DocuSign

**Aditya K Sood, Ph.d**

Advisor, Speaker and Author SecNiche Security Lab

**Tim Chase**

Director of Field Security Collibra

**Parbir Panda**

Enterprise Architect | Management Consulting | Registrar at NID.

**Nabil Zoldjalal**

Director of Cloud Security Darktrace

**Dan Tyrrell**

Manager, Professional Services Cobalt.io

**Tim Chase**

Director of Cybersecurity U.S, Government Contractor

**Kimberly Mentzell**

Adjunct Professor, Capital Technology University

**Jason Gomes**

Cortex Security Architect, Palo Alto Networks

**Eva Benn**

Senior Security PM Manager (Azure, Edge, Platform, Gaming and Devices), Microsoft

**Michele Myauo, Ph.D**

Managing Director & Senior Security Executive, Accenture

## Europe

**Shem Radzikowski**

Chief Security Architect & Researcher, Secburo Labs

**Dmytro Korzhevin**

Threat Intelligence & Interdiction, Ciso Talos

**Shashank Pandey**

Director and Cyber Security Advisor Cytheon Ltd.

**Lior E.**

Director Microsoft Alliance

**Nick Mitropoulos**

Global Security Operations and Security Engineering Manager Confidential

**Sabna Sainudeen**

Director of Applications Security, Carlsberg

## IMEA

**Abhishek Tripathi**

Cyber Security Incident Response and Forensics Reserve Bank Information Technology

**Akansha Mishra**

Information Security Business Partner Amdocs

**Aghiath Chbib**

Chief Executive Officer Seecra

**Amit Ghodekar**

SVP & CISO Motilal Oswal Financial Services Ltd.

**Hamad Al Katheri**

VP of Enterprise Risk & Information Security Zain KSA

**Manoj Arora**

AVP-Information Security Religare Finvest Limited (SME Loans)

**Roshdi A. Osman**

Cybersecurity Strategist Saudi Aramco

**Vikram Mehta**

Founder & CEO Cy5.io

**Pappu Mandal**

Associate, Cognizant

**Abhishek Anand**

Associate Director TAC Security

**Ravinder Arora**

Chief Information Security Officer IRIS Software Inc.

**Aditya Khullar**

Risk Management | Data Privacy | Audits, Indigo Airlines

**Mainak Biswas**

Chief Information Security Officer (CISO), Emkay Global financial Services Ltd.

**Tapan Jha Kumar**

Penetration Tester ASDN Cybernetics Ins.

**Shaikh J Ahmed**

Head Information Security Renault Nissan Technology and Business Center India

**Sudipta Biswas**

VP & CISO Prime Infoserv

**Siddesh Shenvi**

Title Deputy Vice President-Internal Audit Axis Bank

**Mohamed Saad Mousa**

Head of information security (CISO), IKEA Saudi Arabia

**Ahmed Algain**

Management Information System. CyberSecurity-Technology Consulting Independent Saudi Arabia, KSA

## Europe

**Carter Tan**

Solutions Architect Ensign InfoSecurity

EC-Council

Building A Culture Of Security

www.eccouncil.org