EHGI

Ethical Hacker Group International

www.ehgi.nl

TABLE OF CONTENTS

Executive Summary

Problem Statement

Proposed Solution

Methodology

Scope and Timeline

The Team

Projects

Capabilities

Technology and Tools

Client Testimonials

Executives

Consultants

Key Metrics

Services

EXECUTIVE SUMMARY

Ethical Hacker Group International (EHGI), headquartered in Amsterdam, Netherlands, is a premier cybersecurity firm specializing in comprehensive penetration testing and security assessments. Our mission is to safeguard organizations from the dynamic and ever-evolving landscape of cyber threats by delivering thorough and effective security solutions. With a team of highly qualified professionals, we ensure our clients can operate securely and with confidence.

We address the increasing global cybersecurity threats with a focus on vulnerabilities faced by organizations worldwide. Our proposed solution includes extensive penetration testing and security assessments across various domains such as network infrastructure, Active Directory, web applications, software, and cloud environments. Our methodology adheres to industry standards, ensuring comprehensive and systematic security evaluations.

Our team consists of highly experienced professionals holding prestigious certifications and a proven record of success across multiple sectors. We have successfully completed major projects for banks, government entities, healthcare institutions, and other critical infrastructures. EHGI's leadership comprises experts in cybersecurity, driving the firm's mission to enhance cybersecurity standards globally.

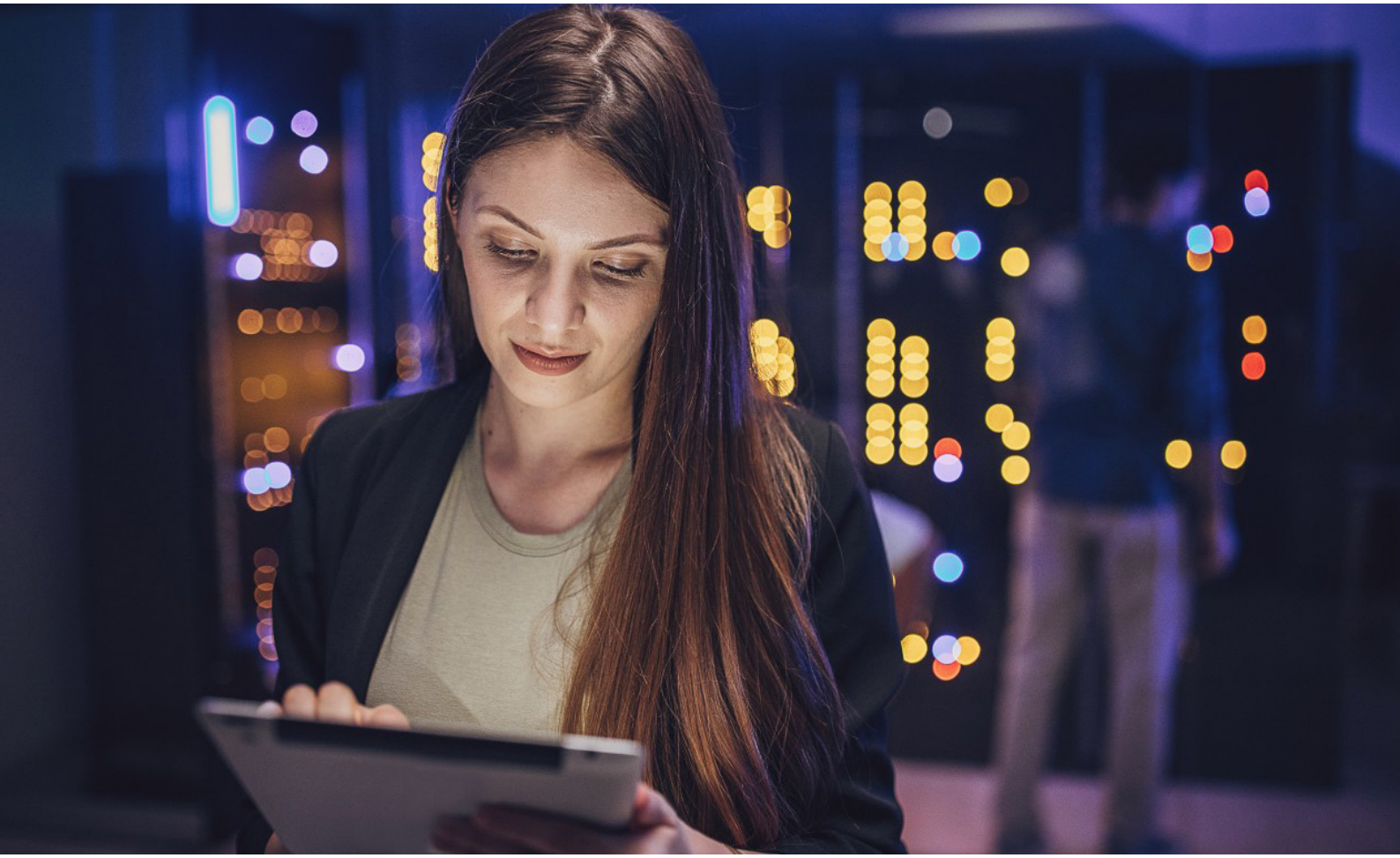
EHGI

PROBLEM STATEMENT

Cybersecurity threats have surged globally, posing significant risks to digital operations. Organizations around the world are increasingly targeted by sophisticated cyberattacks that compromise critical data, disrupt operations, and damage reputations. These attacks exploit vulnerabilities in internet-facing applications, such as websites, email servers, VPNs, firewalls, cloud applications, and databases. Each exposed asset increases the risk of unauthorized access and potential breaches.

Compounding these concerns is the frequent discovery of organizational credentials and sensitive company data on the dark web. The availability of such information facilitates unauthorized access by cybercriminals who leverage stolen credentials to penetrate networks. It is crucial to recognize that hackers can always identify all internet-facing applications an organization owns, including websites, servers, login pages, and email accounts. Since the internet exposes these resources, they must be rigorously protected to prevent unauthorized access and potential data breaches.

Additionally, organizations have valuable systems that are critical to their operations and must remain online at all times. Cybercriminals often target these systems to shut them down, forcing companies to halt operations, leading to significant financial losses and operational disruptions. Furthermore, hackers frequently leak classified information that organizations strive to keep private, exacerbating the damage by exposing sensitive data to the public and competitors. This dual threat of operational disruption and data leakage underscores the urgent need for robust cybersecurity measures.



EHGI

PROPOSED SOLUTION

To address the comprehensive cybersecurity needs of your organization, we propose a multifaceted approach encompassing a variety of our specialized services. Our solution involves conducting extensive penetration tests across all internet-facing applications and internal systems, ensuring rigorous evaluation and uncovering potential vulnerabilities. Our primary services include:

Penetration Testing Services

✓ Network Pentest

Comprehensive testing of your network infrastructure to identify and mitigate vulnerabilities.

✓ Active Directory Pentest

Specialized assessment of your Active Directory to ensure robust security configurations.

✓ Web Application Pentest

Detailed evaluation of web applications to uncover security weaknesses and protect against threats.

✓ Software Pentest

In-depth analysis of your software applications to identify and address security issues.

✓ Cloud Pentest

Security testing of cloud environments to ensure safe and compliant cloud operations.

✓ Zero Measurement

Baseline security assessment to understand current security posture and identify areas for improvement.

Consultancy and Advisory Services

✓ Cyber Consultancy

Expert advice and support to enhance your overall cybersecurity strategy.

✓ Identity and Access Management

Ensuring secure access controls and management of user identities to protect sensitive information.

Managed Security Services

✓ Security Operations Center (SOC) Services

Comprehensive SOC services including 24/7 monitoring, threat detection, incident response, vulnerability management, and compliance support.

✓ Vulnerability Management

Proactive identification, assessment, and mitigation of security vulnerabilities to minimize risk exposure.

Training and Awareness

✓ International Cybersecurity Training Service

Training programs to enhance cybersecurity awareness and skills among employees.

Insurance Services

✓ Cybersecurity Insurance Readiness Service

Assisting your organization in meeting the criteria for cybersecurity insurance coverage through comprehensive testing, monitoring, and continuous improvement measures.

This comprehensive approach ensures robust protection against a wide array of cyber threats, enhancing your overall security posture and enabling your organization to operate securely.

EHGI

METHODOLOGY

Our methodology for each service ensures a thorough and systematic security assessment, tailored to address the specific needs of your organization's infrastructure.

Principle & Standards

The security assessments are performed based on industry-standard frameworks such as the OWASP Web Security Testing Guide (WSTG) for web applications, CIS benchmarks for Active Directory, and other relevant standards for network and cloud environments. This approach ensures comprehensive coverage and compliance with best practices in cybersecurity.

Testing Approach

We adopt a combination of Black box, Grey box, and White box testing approaches depending on the service and specific requirements:

- **Black Box Testing:** Simulates an external attack without prior knowledge of the internal workings. This is particularly useful for assessing the security of internet-facing applications.
- **Grey Box Testing:** Combines partial knowledge of the internal environment with external testing techniques to uncover vulnerabilities more effectively.
- **White Box Testing:** Involves a detailed examination of internal structures, including code reviews, to identify security weaknesses from within.

High-Level Steps to Testing:

1 Reconnaissance and Enumeration

Gathering data about targeted systems using industry-standard tools, including network scanning and dark web analysis to identify compromised credentials.

2 Vulnerability Analysis

Utilizing automated scanners and manual analysis to detect vulnerabilities ranging from known exploits to undiscovered security flaws.

3 Exploitation

Validating identified vulnerabilities by attempting to exploit them, thus confirming their presence and potential impact.

4 Post-Exploitation

Analyzing successful exploitations to understand the extent of potential damage, including unauthorized data access and privilege escalation.

5 Reporting

Documenting findings in a detailed report, outlining the associated risks of each vulnerability, verifying successful exploitations, and recommending strategic remediation measures. This report is tailored for both technical teams and executive management.

6 Client Communication and Follow-Up

Maintaining transparent communication throughout the engagement, offering clarifications on findings, and assisting in prioritizing remediation steps. Providing post-remediation re-testing to confirm vulnerabilities have been addressed.

7 Cyclical Testing

Emphasizing the importance of periodic testing to maintain a high level of security, with quarterly testing services available to continually assess and enhance your security posture.

EHGI

SCOPE AND TIMELINE

Example scope and timeline for a Web-Application Pentest:

#	Test Type	Scope	Time	Deliverables
1	Initial Test	Internet-facing application & Leaked credentials	48 hours	Initial pentest report including remediations
2	Complete in-depth pentest	Internet-facing application & Leaked credentials	Based on the initial test	Complete pentest report including remediations
3	Consulting for solving found issues (Online). - Customer Support	Internet-facing application & Leaked credentials	On-Demand	On-demand consultation
4	Complete re-test of all systems	Internet-facing application & Leaked credentials	Based on the pentest	Re-test pentest report including remediations
5	Repeat 2-4	Quarterly		

EHGI

THE TEAM

As a professional collective of cybersecurity experts, our team boasts a blend of experience, expertise, and qualifications dedicated to safeguarding critical high-stake infrastructures like those of banks, governments, and corporations. With a proven record of excellence, we stand poised to deliver comprehensive solutions tailored to your specific cybersecurity needs.

Professional Experience

Our collective experience spans over 50 major projects in penetration testing and vulnerability assessment across diverse sectors ranging from banking to government and healthcare. We have conducted comprehensive assessments, digital forensics investigations, and security compliance activities aligning with stringent standards such as HIPAA, CCPA, CPRA, and ISO 27001.

Qualifications and Certifications

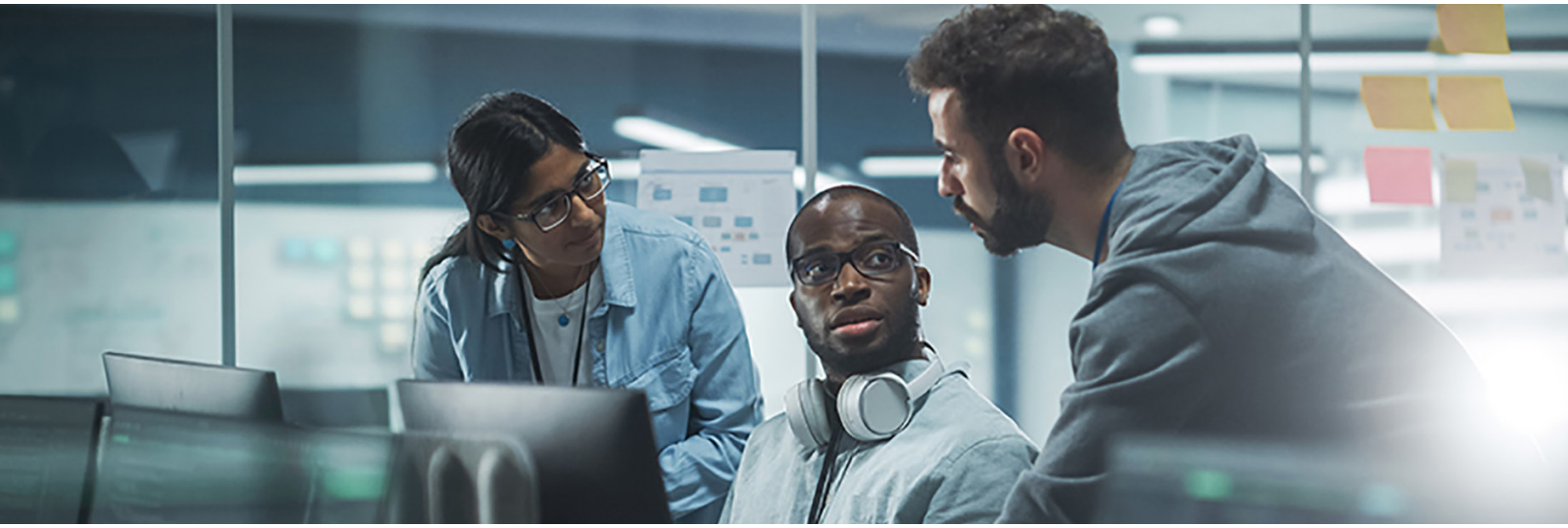
Our team members hold esteemed certifications that underscore our proficiency in cybersecurity:

- Offensive Security Certified Professional (OSCP)
- Offensive Security Experienced Penetration Tester (OSEP)
- Elearn Security Certified Pentester (ECPPTv2)
- Web application Penetration Tester eXtreme (eWPTX)
- Certified Professional Penetration Tester | INE Security
- Certified Ethical Hacker | EC-council
- CSFPC | Certiprof
- IBM QRADAR SIEM solution training by Ebryx
- PCI-DSS compliance training by RISK ASSOCIATES
- Certified Information Systems Security Professional (CISSP)

Moreover, our team has honed its skills through rigorous training and participation in competitive scenarios:

- Demonstrated excellence with top rankings in renowned Capture the Flag (CTF) competitions such as Ignite and UET
- Specialized training encompassing Cloud Security, Cyber Risk, Application Security, and expertise in compliance frameworks like PCI-DSS

With a proven record of success and a commitment to excellence, our team stands ready to partner with your organization in fortifying its cybersecurity defenses and protecting its critical assets against evolving threats. We look forward to transforming your organization into a cyber-secure entity.



EHGI

GWAPT

GXPN

OSEP

PenTest+

EC-Council CERTIFIED CEH

CISA

CISM

CySA+

OSCP

INE SECURITY

CISSP Certified Information Systems Security Professional

CEH Certified Ethical Hacker

Risk Associates

CertiProf Professional Knowledge

PCI DSS COMPLIANT

ebryx

Get certified in Cyber Security Foundations

EC-Council

eWPTX V2

eCPPT V2

OFFENSIVE security

eCPPT

CBBH

CPTS

EHGI

PROJECTS

Our team possesses extensive experience in the field of penetration testing and cybersecurity, trusted by banks, government entities, healthcare institutions, and SMBs in the Netherlands and around the globe. Leveraging comprehensive knowledge and advanced techniques, we have successfully safeguarded critical infrastructures and sensitive data for prestigious clients such as Rabobank, the Bank of Punjab, and numerous others across various sectors. Here are some of our key projects and achievements:

Multiple Cloud and Web-Application Vulnerability Assessments
Performed comprehensive vulnerability assessments for Rabobank, the second-largest bank in the Netherlands, focusing on enhancing security protocols and identifying potential threats.

Network and Location Penetration Testing for Amsterdam Municipality
Conducted extensive penetration testing across multiple networks and physical locations to secure the digital and physical infrastructures of the Amsterdam municipality.

Hospital Penetration Testing in the Netherlands
Executed critical security penetration tests for a major hospital in the Netherlands, ensuring compliance with healthcare regulations and safeguarding sensitive medical data against cyber threats.

PCI DSS Compliance and Security Deployments at The Bank of Punjab
Guided PCI DSS compliance and other security deployment projects, including the implementation of Enhanced Data Rate (EDR) and endpoint solutions, as well as Static and Dynamic Application Security Testing (SAST/DAST) solutions.

SMB Penetration Testing in the Netherlands
Delivered penetration testing solutions for multiple Small and Medium-sized Businesses (SMBs), enhancing their security posture against emerging cyber threats.

Terra Virtua Marketplace Penetration Testing (Web3)
Conducted targeted penetration testing of the blockchain-based Terra Virtua Marketplace to identify and rectify vulnerabilities in this digital landscape.

NITRO Racing Game and Supporting Infrastructure Penetration Testing
Carried out comprehensive security assessments of NITRO's racing game, including its backend, frontend, API, mobile, and decentralized application (DAPP) components.

Fintech Web Application and Infrastructure Penetration Testing
Performed assessments and penetration testing of web applications and infrastructure in the fintech sector, including robust testing of Amazon Web Services hosted environments.

Development and Training Initiatives
Created and revised policies and Standard Operating Procedures (SOPs) focusing on industry-standard security practices. Facilitated secure code development workshops for developers at Tkxel and conducted specialized security training for developers at The Bank of Punjab.

Government and Regulatory Compliance Initiatives
Executed deployment projects for government initiatives, such as the Roshan Digital Account at The Bank of Punjab, aligning with national financial inclusion strategies and securing banking operations.

Web application pentest for NOC Libya
Conducted an in-depth web application penetration test for the National Oil Corporation (NOC) of Libya. The assessment identified critical vulnerabilities, provided remediation strategies, and enhanced the overall security posture of their web applications, ensuring robust protection against potential cyber threats.

Active Directory and Network Pentest for PCOU Willibrord
Conducted comprehensive penetration testing for PCOU Willibrord, a major education organization overseeing approximately 50 schools in the Netherlands, identifying critical vulnerabilities and enhancing security protocols.

Zuyderland Hospital in the Netherlands
Performed infrastructure and network penetration testing for Zuyderland Hospital, ensuring compliance with healthcare regulations and safeguarding sensitive medical data against cyber threats.

Municipality of Amsterdam
Conducted multiple penetration tests for the Municipality of Amsterdam, securing their digital and physical infrastructures.

Sirt Oil
Performed web application penetration testing for Sirt Oil, identifying and mitigating critical vulnerabilities.

EHGI

zuyderland

pcou willibrord

FIDUZIA
UITZENDBUREAU

tkxel
technology accelerated
to deliver.

IT ZAKEN
DOELGERICHT NAAR DE BESTE OPLOSSING

City of
Amsterdam

BOP
THE BANK OF PUNJAB

Rabobank

EHGI

CAPABILITIES

EHGI boasts the ability to host two weekly seminars for the students in our hacking group, which has over 500 members. We have a large pool of some of the Netherlands' best hackers to choose from and employ for major projects worldwide. We also work with international ethical hackers to provide the best services. Our organization can manage more than 50 large scale projects concurrently while offering high-level customer service.

EHGI

TECHNOLOGY AND TOOLS

EHGI utilizes the most up-to-date technology and continuously improves our practices. We work with a variety of industry-leading tools and software to ensure comprehensive and effective cybersecurity measures. We are committed to learning and adopting new technologies to stay ahead of emerging threats.

Microsoft
tenable
okta
Office 365
vmware
PortSwigger
SentinelOne
Microsoft Azure
aws
CROWDSTRIKE
Google Cloud
BURPSUITE PROFESSIONAL
IBM Radar
splunk>
COBALT STRIKE
zscaler
paloalto NETWORKS
CYBERARK
CORE IMPACT CORE SECURITY
LogRhythm The Security Intelligence Company
CISCO FirePower
FORTINET
SOPHOS

EHGI

CLIENT TESTIMONIALS

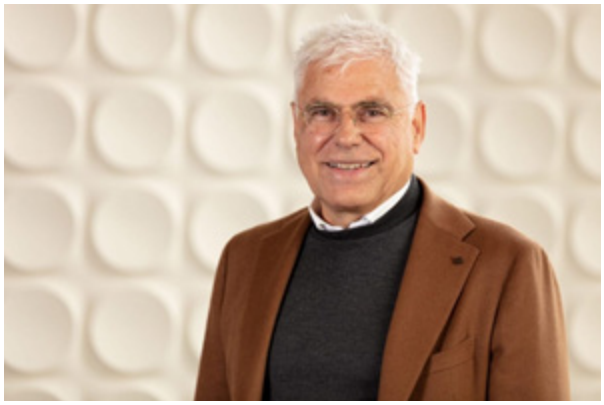
EHGI boasts the ability to host two weekly seminars for the students in our hacking group, which has over 500 members. We have a large pool of some of the Netherlands' best hackers to choose from and employ for major projects worldwide. We also work with international ethical hackers to provide the best services. Our organization can manage more than 50 large scale projects concurrently while offering high-level customer service.

> EHGI has demonstrated an excellent ability to translate our security test assignment into the desired execution. They presented their findings in clear language and with a clear explanation. Based on this report, we can implement several improvements.
>
> — Jeroen van Maanen, Information Security & Privacy Advisor at PCOU Willibrord

pcou willibrord

> EHGI has proven to work very professionally and conducted the penetration test exceptionally well. Their expertise and thorough approach ensured that all aspects of our security were meticulously examined.
>
> — Wim van Deijzen, Founder and CEO, VCS Observation

VCS
Samen werken aan veiligheid



EHGI has been an outstanding partner in our cybersecurity efforts. Their professional approach and deep expertise have significantly enhanced our security posture. The comprehensive penetration test they conducted was executed with meticulous attention to detail, and the insights provided were invaluable. We highly recommend their services to any organization looking to bolster their cybersecurity defenses.

— Ranjeet Gajadhar, Founder and CEO, Fiduzia

FIDUZIA
UITZENDBUREAU

EXECUTIVES

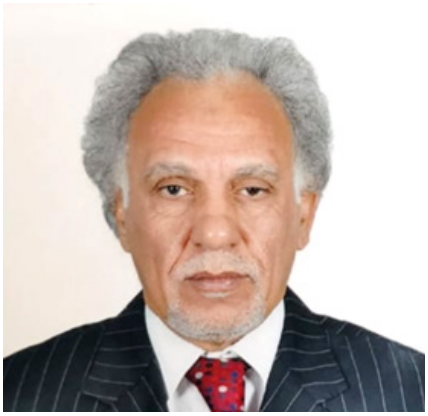
Anass Ali - General Director

Anass Ali is the General Director of Ethical Hacker Group. With a broad and extensive background in penetration testing and cybersecurity, Anass has established himself as a leading figure in the industry both in the Netherlands and on international projects. His expertise encompasses a wide range of security assessments, from network to web applications and cloud environments. Anass also leads a formidable team of 500 ethical hackers, guiding and mentoring them to excel in the field. His commitment to advancing cybersecurity standards and his proactive approach to threat mitigation make him a pivotal asset to our organization.

Email: Anass.Ali@ehgi.nl
Phone: +31 6 421 978 03

EHGI

Mohamed Bin Othman - Marketing Director



Mohamed Bin Othman serves as the Marketing Director at Ethical Hacker Group. As a seasoned entrepreneur, Mohamed brings a wealth of experience in international business, marketing, and deal-making to the table. His strategic insight and innovative approach have been instrumental in driving our market presence and expanding our reach globally. Mohamed's expertise in crafting impactful marketing campaigns and forging strategic partnerships has significantly contributed to the growth and success of our firm.

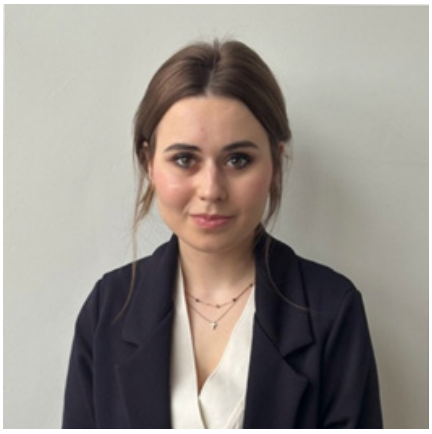
Email: Mohamed.BinOthman@ehgi.nl
Phone: +31 6 421 978 02 (Whatsapp)
Phone: +218 9 121 315 44

CONSULTANTS

Lidia M. Pérez Leutza – Consultant

Lidia is a skilled Business Technology Analyst at Capgemini, specializing in cybersecurity and IT business solutions. Based in The Randstad, Netherlands, she has significant experience in cybersecurity consulting, information and change management, and customer due diligence.

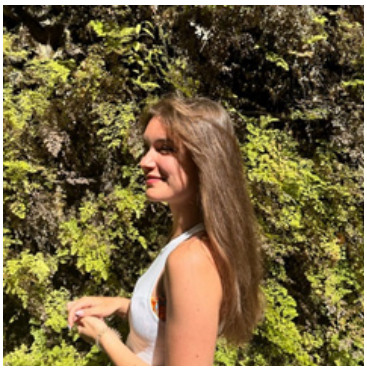
She has delivered impactful solutions at organizations such as Capgemini, BECIS | DIOR, SEPAY BV, and ECT Rotterdam. At EHGI, we consult Lidia on cybersecurity matters. Her extensive background and proactive approach make her a valuable resource for our team, helping to drive our mission to enhance cybersecurity standards globally.



Lois Vosmeer

Lois is a Cyber Security Consultant at CGI with a strong background in cybersecurity and business IT management. Based in Amsterdam, North Holland, she has extensive experience in cybersecurity consulting, ICT legislation, compliance, and governance. Lois has worked on various projects, including ITIL to Agile transitions and secure configuration management, at prominent institutions such as the University of Amsterdam and the City of Amsterdam. Her work focuses on integrating IT solutions to enhance organizational efficiency and security.

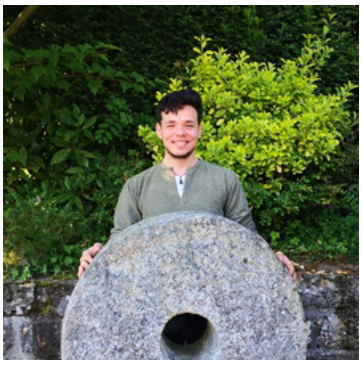
At EHGI, Lois contributes her deep expertise in cybersecurity. Her ability to navigate complex security challenges and provide strategic insights is invaluable to our efforts in advancing cybersecurity measures and protecting critical assets.



Nekija Džemaili

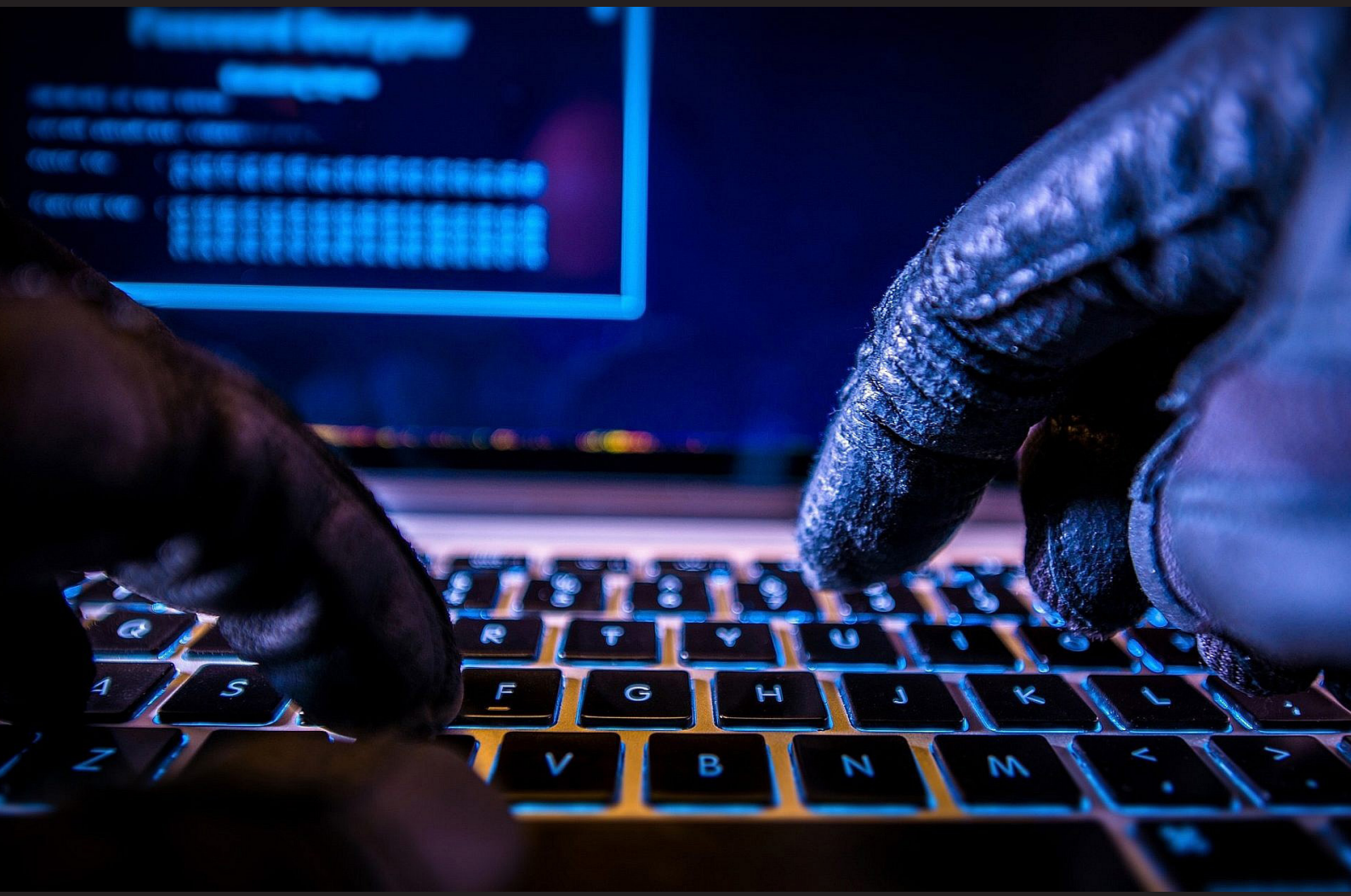
Nekija is currently pursuing an MSc in Electrical Engineering at the University of Twente. With previous experience at CERN in Geneva, he brings a wealth of knowledge in dependable integrated systems, integrated circuit design, and robotics. Nekija is passionate about tackling complex problems and pushing the boundaries of his field. He has worked on various projects, including designing PCBs and embedded systems, and has experience as a teaching assistant in programming and software development for robotics. His role at RISE - UT/VU Student Team and University of Twente has honed his skills in both practical and theoretical aspects of electrical engineering.

At EHGI, Nekija's expertise in electrical engineering and integrated systems greatly enhances our technical capabilities. His innovative approach and hands-on experience in cutting-edge technologies are instrumental in driving our advanced cybersecurity solutions.



KEY METRICS

251,237 Total Vulnerabilities Found	**75,483** Unique Vulnerabilities Found	**45,926** Critical Vulnerabilities Found
501,764 Systems Analyzed	**225,318** Vulnerabilities Patched	**300,752** Security Recommendations Made



EHGI

SERVICES

PENETRATION TESTING SERVICES

Network Pentest

Problem

Your company uses a network infrastructure but is unsure if it has the proper configurations and if there are vulnerabilities that could be exploited.

Solution

By using our Network Pentest service, we provide a comprehensive evaluation of your network infrastructure to identify and mitigate vulnerabilities. This includes identifying open ports and services, evaluating network configurations, and simulating real-world attacks to uncover weaknesses. Our experts use advanced tools such as Nmap, Nessus, and Metasploit to ensure your network's security and integrity.

Service Details

Our Network Pentest involves:

- Identifying open ports and services
- Evaluating network configurations
- Testing for weak points in firewall defenses
- Simulating real-world attacks to uncover vulnerabilities
- Using advanced tools such as Nmap, Nessus, and Metasploit

Benefits

- Enhanced security posture
- Identification and remediation of vulnerabilities
- Improved compliance with industry standards
- Increased resilience against cyber attacks

Process

1. Reconnaissance: Gathering information about the network using tools like Nmap and Nessus.
2. Vulnerability Scanning: Using automated scanners to detect potential weaknesses.
3. Exploitation: Attempting to exploit identified vulnerabilities to assess their impact.
4. Reporting: Providing a detailed report with findings and remediation recommendations.
5. Remediation Support: Assisting in the implementation of remediation measures.
6. Re-testing: Re-assessing the network to ensure vulnerabilities have been addressed.

Contact Information

For more information about our Network Pentest service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

Active-Directory Pentest

Problem

Your company uses Active Directory but is unsure if the proper configurations are used and if there are vulnerabilities that could be exploited.

Solution

Our Active-Directory Pentest service assesses the security of your Active Directory infrastructure. We evaluate configurations, test for weak password policies, assess user and group permissions, and identify potential misconfigurations and vulnerabilities using tools like BloodHound and PowerView. This ensures robust security configurations, improved access control, and compliance with industry standards.

Service Details

Our Active-Directory Pentest includes:

- Evaluating AD configurations and policies
- Testing for weak password policies
- Assessing user and group permissions
- Identifying potential misconfigurations and vulnerabilities
- Utilizing tools such as BloodHound and PowerView

Benefits

- Improved AD security configurations
- Detection and remediation of vulnerabilities
- Enhanced access control and user management
- Compliance with industry standards

Process

1. Reconnaissance: Collecting information about the AD environment.
2. Configuration Analysis: Assessing AD configurations and policies.
3. Vulnerability Scanning: Using tools to detect weak points.
4. Exploitation: Attempting to exploit identified vulnerabilities.
5. Reporting: Delivering a detailed report with findings and recommendations.
6. Remediation Support: Assisting in implementing security improvements.
7. Re-testing: Ensuring vulnerabilities have been mitigated.

Contact Information

For more information about our Active-Directory Pentest service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

EHGI

Web-Application Pentest

Problem

Your company relies on web applications but is unsure if they have the proper security measures in place and if there are vulnerabilities that could be exploited.

Solution

With our Web-Application Pentest service, we identify and mitigate vulnerabilities within your web applications. Using OWASP standards, we assess vulnerabilities like SQL injection, XSS, and CSRF, test authentication and authorization mechanisms, and evaluate input validation and error handling. Tools like Burp Suite, OWASP ZAP, and Nikto help us provide a detailed evaluation to protect your web presence.

Service Details

Our Web-Application Pentest involves:

- Assessing web application security using OWASP standards
- Identifying vulnerabilities such as SQL injection, XSS, and CSRF
- Testing authentication and authorization mechanisms
- Evaluating input validation and error handling
- Using tools like Burp Suite, OWASP ZAP, and Nikto

Benefits

- Improved web application security
- Identification and remediation of vulnerabilities
- Protection against common web attacks
- Compliance with industry standards

Process

1. Reconnaissance: Gathering information about the web applications.
2. Vulnerability Scanning: Using tools to detect potential vulnerabilities.
3. Exploitation: Attempting to exploit identified vulnerabilities.
4. Reporting: Providing a detailed report with findings and recommendations.
5. Remediation Support: Assisting in fixing the identified issues.
6. Re-testing: Verifying that vulnerabilities have been mitigated.

Contact Information

For more information about our Web-Application Pentest service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

Software Pentest

Problem

Your company develops software applications but is unsure if they are secure and free from vulnerabilities that could be exploited.

Solution

Our Software Pentest service assesses the security of your software applications. We review application source code, identify security flaws, and test for issues like buffer overflows and input validation errors using static and dynamic analysis tools. This service ensures enhanced software security and protection against exploitation.

Service Details

Our Software Pentest includes:

- Reviewing application source code
- Identifying security flaws and vulnerabilities
- Testing for buffer overflows, input validation errors, and other issues
- Utilizing static and dynamic analysis tools
- Conducting manual code reviews

Benefits

- Enhanced software security
- Identification and remediation of security flaws
- Protection against exploitation
- Compliance with security standards

Process

1. Reconnaissance: Collecting information about the software application.
2. Code Review: Analyzing source code for security issues.
3. Vulnerability Scanning: Using automated tools to detect vulnerabilities.
4. Exploitation: Attempting to exploit identified issues.
5. Reporting: Delivering a detailed report with findings and recommendations.
6. Remediation Support: Assisting in fixing identified security flaws.
7. Re-testing: Ensuring vulnerabilities have been addressed.

Contact Information

For more information about our Software Pentest service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

EHGI

Cloud Pentest

Problem

Your company utilizes cloud environments but is unsure if the configurations are secure and if there are vulnerabilities that could be exploited.

Solution

The Cloud Pentest service evaluates the security of your cloud environments. We test for misconfigurations, assess access controls, and utilize tools like ScoutSuite and Prowler to conduct security reviews for AWS, Azure, and Google Cloud environments. This ensures secure, compliant, and resilient cloud operations.

Service Details

Our Cloud Pentest includes:

- Evaluating cloud configurations and policies
- Testing for misconfigurations and vulnerabilities
- Assessing access controls and identity management
- Using tools like ScoutSuite and Prowler
- Conducting security reviews for AWS, Azure, and Google Cloud environments

Benefits

- Enhanced cloud security
- Identification and remediation of vulnerabilities
- Improved compliance with cloud security standards
- Increased resilience against cyber attacks

Process

1. Reconnaissance: Gathering information about the cloud environment.
2. Configuration Analysis: Assessing cloud configurations and policies.
3. Vulnerability Scanning: Using tools to detect potential issues.
4. Exploitation: Attempting to exploit identified vulnerabilities.
5. Reporting: Providing a detailed report with findings and recommendations.
6. Remediation Support: Assisting in fixing identified issues.
7. Re-testing: Ensuring vulnerabilities have been mitigated.

Contact Information

For more information about our Cloud Pentest service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

Zero Measurement

Problem

Your company needs to understand its current security posture and identify areas for improvement but lacks a baseline assessment.

Solution

Our Zero Measurement service provides a baseline security assessment to understand your current security posture and identify areas for improvement. This involves conducting a comprehensive security assessment, identifying existing vulnerabilities, and evaluating current security policies and procedures. This establishes a starting point for ongoing security enhancements.

Service Details

Our Zero Measurement service includes:

- Conducting a comprehensive security assessment
- Identifying existing vulnerabilities and security gaps
- Evaluating current security policies and procedures
- Using a combination of automated tools and manual techniques

Benefits

- Establishing a baseline for security improvements
- Identification of vulnerabilities and security gaps
- Enhanced understanding of current security posture
- Guidance for future security initiatives

Process

1. Reconnaissance: Gathering information about the current security posture.
2. Vulnerability Scanning: Using tools to detect existing vulnerabilities.
3. Analysis: Evaluating current security policies and procedures.
4. Reporting: Providing a detailed report with findings and recommendations.
5. Remediation Support: Assisting in implementing security improvements.
6. Re-assessment: Conducting periodic re-assessments to measure progress.

Contact Information

For more information about our Zero Measurement service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

EHGI

CONSULTANCY AND ADVISORY SERVICES

Cyber Consultancy

Problem

Your company requires expert guidance to enhance its cybersecurity strategy and mitigate risks effectively.

Solution

Our Cyber Consultancy service offers expert advice and support to develop robust security measures. We conduct risk assessments, develop security policies, provide guidance on compliance, and offer strategic advice on cybersecurity investments. This service ensures enhanced security strategy and reduced risk of cyber threats.

Service Details

Our Cyber Consultancy service includes:

- Conducting risk assessments and security audits
- Developing and implementing security policies and procedures
- Providing guidance on compliance with industry standards
- Offering strategic advice on cybersecurity investments
- Delivering tailored security training and awareness programs

Benefits

- Expert guidance on cybersecurity best practices
- Enhanced security strategy and policies
- Improved compliance with industry standards
- Reduced risk of cyber threats

Process

1. Consultation: Understanding the client's cybersecurity needs and objectives.
2. Assessment: Conducting risk assessments and security audits.
3. Strategy Development: Developing tailored security strategies and policies.
4. Implementation: Assisting in the implementation of security measures.
5. Training: Providing security training and awareness programs.
6. Ongoing Support: Offering continuous support and guidance.

Contact Information

For more information about our Cyber Consultancy service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

Identity and Access Management

Problem

Your company needs to ensure secure access to resources and manage user identities effectively to protect sensitive information.

Solution

Our Identity and Access Management (IAM) service implements secure identity verification processes, sets up role-based access controls, and ensures secure authentication mechanisms. Tools like Okta, Azure AD, and AWS IAM are used to provide efficient management of user identities and permissions, ensuring secure access to your organization's resources.

Service Details

Our IAM service includes:

- Implementing and managing identity verification processes
- Setting up role-based access controls (RBAC)
- Ensuring secure authentication and authorization mechanisms
- Monitoring and auditing user activities
- Using tools like Okta, Azure AD, and AWS IAM

Benefits

- Enhanced security through controlled access
- Improved compliance with industry regulations
- Reduced risk of unauthorized access
- Efficient management of user identities and permissions

Process

1. Assessment: Evaluating current IAM practices and identifying areas for improvement.
2. Design: Developing a tailored IAM strategy based on the assessment.
3. Implementation: Setting up and configuring IAM tools and processes.
4. Training: Providing training for users and administrators.
5. Monitoring: Continuously monitoring IAM activities and making necessary adjustments.
6. Review: Periodically reviewing IAM practices to ensure they remain effective and compliant.

Contact Information

For more information about our Identity and Access Management service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

EHGI

MANAGED SECURITY SERVICES

Security Operations Center (SOC) Services

Problem
Your company needs continuous monitoring and management of security operations to detect and respond to cyber threats in real-time.

Solution
Our Security Operations Center (SOC) services provide 24/7 monitoring and management of your organization's security operations. This service includes threat detection, incident response, vulnerability management, and compliance support, ensuring real-time protection against cyber threats.

Service Details
Our SOC services include:
- 24/7 Monitoring: Continuous monitoring of systems, networks, and applications to identify potential security threats.
- Threat Detection: Advanced capabilities to identify known and unknown threats, including malware, phishing, and DoS attacks.
- Incident Response: Rapid response and remediation of security incidents to minimize business impact.
- Vulnerability Management: Identifying and remediating vulnerabilities to prevent exploitation.
- SIEM: Collection, analysis, and correlation of security data from various sources.
- Compliance Management: Support for compliance with industry standards and regulations such as HIPAA, PCI-DSS, and GDPR.
- Security Consulting: Expert advice on security best practices, risk management, and security strategy.

Benefits
- Real-time threat detection and response
- Enhanced overall security posture
- Improved compliance with industry standards
- Expert guidance and support

Process
1. Initial Consultation: Understanding the client's security requirements and goals.
2. Onboarding: Installing and configuring SOC tools and integrating with the client's infrastructure.
3. Monitoring: Continuous monitoring and threat detection.
4. Incident Response: Rapid response to security incidents.
5. Reporting: Regular reports on security activity and incidents.
6. Review: Periodic reviews to ensure the SOC services are meeting the client's needs.

Contact Information
For more information about our Security Operations Center (SOC) services, please contact:
Email: services@ehgi.nl
Phone: 0031642197803

Vulnerability Management

Problem
Your company needs proactive identification, assessment, and mitigation of security vulnerabilities to minimize risk exposure.

Solution
Our Vulnerability Management service focuses on the proactive identification, assessment, and mitigation of security vulnerabilities. This service includes continuous monitoring, prioritization of vulnerabilities, development and implementation of remediation plans, and regular updates to maintain a strong security posture.

Service Details
Our Vulnerability Management service includes:
- Continuous monitoring and scanning for vulnerabilities
- Prioritization of vulnerabilities based on risk and impact
- Development and implementation of remediation plans
- Regular updates and patches to address identified vulnerabilities
- Reporting and documentation of vulnerability status and remediation progress

Benefits
- Reduced risk of security breaches
- Improved compliance with industry standards
- Enhanced overall security posture
- Proactive identification and remediation of vulnerabilities

Process
1. Scanning: Continuous monitoring and scanning of systems and applications for vulnerabilities.
2. Analysis: Prioritizing vulnerabilities based on risk and potential impact.
3. Remediation: Developing and implementing plans to address identified vulnerabilities.
4. Reporting: Providing detailed reports on vulnerability status and remediation efforts.
5. Ongoing Monitoring: Continuously monitoring systems and applications to identify new vulnerabilities.
6. Re-assessment: Periodically re-assessing systems to ensure vulnerabilities have been mitigated.

Contact Information
For more information about our Vulnerability Management service, please contact:
Email: services@ehgi.nl
Phone: 0031642197803

EHGI

TRAINING AND AWARENESS

International Cybersecurity Training Service

Our Cybersecurity Training service offers international, on-premise training programs, including in the Netherlands and Turkey. We provide comprehensive training to enhance cybersecurity awareness and skills among employees, tailored to meet your organizational needs.

Problem

Your company needs to enhance cybersecurity awareness and skills among employees to build a security-conscious culture.

Solution

Our Cybersecurity Training service provides comprehensive training programs designed to enhance cybersecurity awareness and skills among employees. This service includes security awareness training, specialized training for IT and security professionals, hands-on workshops, and compliance training, tailored to meet your organizational needs.

Service Details

Our Cybersecurity Training includes:

- Security awareness training for employees
- Specialized training for IT and security professionals
- Hands-on workshops and simulation exercises
- Training on compliance requirements and best practices
- Customized training programs tailored to specific organizational needs

Benefits

- Improved cybersecurity awareness among employees
- Enhanced skills and knowledge of IT and security teams
- Increased resilience against cyber threats
- Compliance with training requirements of industry standards

Process

1. Needs Assessment: Identifying the training needs of the organization.
2. Program Development: Developing customized training programs based on the assessment.
3. Delivery: Conducting training sessions through various formats (in-person, online, workshops).
4. Evaluation: Assessing the effectiveness of the training programs.
5. Ongoing Support: Providing continuous support and updates to the training content.

Training Programs Offered

EC-Council:

- Certified Ethical Hacker v12 (CEHv12)
- Certified Ethical Hacker Master training
- Certified SOC Analyst (CSA)
- Certified Hacking Forensic Investigator (CHFI)
- Certified Incident Handler (ECIH)
- Certified Network Defender v2 (CND)

ISC2:

- Certified in Cybersecurity (CC)
- Systems Security Certified Practitioner (SSCP)
- Certified Information Systems Security Professional (CISSP)
- CISSP English Course
- Certified Cloud Security Professional (CCSP)

ISACA:

- Certified Information Security Manager (CISM)
- Certified Information System Auditor (CISA)

Microsoft:

- AZ 104 Microsoft Azure Administrator
- AZ 500 Microsoft Azure Security Technologies
- AZ 900 Microsoft Azure Fundamentals
- MS 900 Microsoft 365 Fundamentals
- SC 200 Microsoft Security Operations Analyst
- SC 900 Security, Compliance, and Identity Fundamentals

Additional Certifications and Workshops:

- Offensive Security Certified Professional (OSCP)
- Hacking Essentials
- Kali Linux for Hackers

Contact Information

For more information about our Cybersecurity Training service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

EHGI

INSURANCE SERVICES

Cybersecurity Insurance Readiness Service

Our Cybersecurity Insurance Readiness Service is designed to help your organization meet the criteria for cybersecurity insurance coverage. This comprehensive package includes testing, monitoring, and other essential services to ensure your organization is well-prepared to secure and maintain cybersecurity insurance.

Problem

Many organizations face difficulties in meeting the stringent criteria required for cybersecurity insurance coverage. Without proper preparation and ongoing management, obtaining and retaining insurance can be challenging and costly.

Solution

Our Cybersecurity Insurance Readiness Service provides a bundled solution to help your organization meet the necessary criteria for cybersecurity insurance. This service includes comprehensive testing, monitoring, and continuous improvement measures to ensure your organization is always prepared.

Service Details

Our Cybersecurity Insurance Readiness Service includes:

Penetration Testing
Conduct thorough penetration testing to identify and address vulnerabilities.

Security Monitoring
Implement continuous security monitoring to detect and respond to threats in real-time.

Compliance Audits
Perform regular compliance audits to ensure adherence to industry standards and insurance requirements.

Incident Response Planning
Develop and test incident response plans to ensure readiness in the event of a cybersecurity incident.

Employee Training
Provide ongoing training for employees on cybersecurity best practices and awareness.

Policy and Procedure Development
Assist in developing and updating cybersecurity policies and procedures to meet insurance criteria.

Benefits

Improved Security Posture
Enhance your organization's overall security posture through comprehensive testing and monitoring.

Insurance Compliance
Ensure your organization meets the necessary criteria for cybersecurity insurance coverage.

Cost Savings
Reduce the risk of costly breaches and insurance premiums through proactive security measures.

Peace of Mind
Gain confidence in your organization's ability to secure and maintain cybersecurity insurance coverage.

Process

1. Initial Assessment
Conduct an initial assessment to identify your organization's current security posture and insurance requirements.

2. Program Development
Develop a customized program based on the assessment to meet insurance criteria.

3. Implementation
Implement the necessary security measures, including testing, monitoring, and training.

4. Evaluation
Evaluate the effectiveness of the implemented measures and make necessary adjustments.

5. Ongoing Support
Provide continuous support and updates to ensure ongoing compliance and readiness.

Contact Information

For more information about our Cybersecurity Insurance Readiness Service, please contact:

Email: services@ehgi.nl
Phone: 0031642197803

By choosing our Cybersecurity Insurance Readiness Service, your organization can confidently meet the criteria for cybersecurity insurance, ensuring comprehensive protection against cyber threats.

EHGI

EHGI

Our practices follow the highest standards ensuring responsible and secure solutions.

Contact Us

+31 6 421 978 03 | info@ehgi.nl | www.ehgi.nl