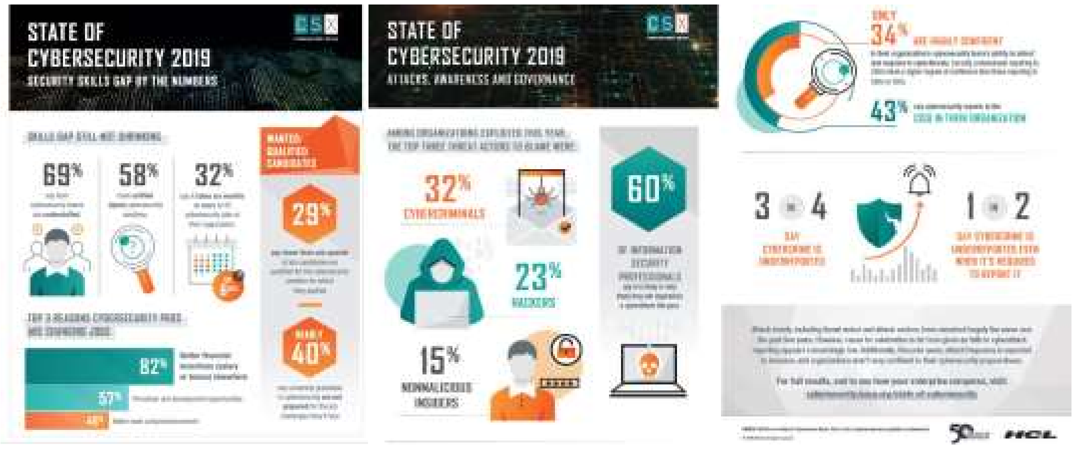
SCORPIONSHIELD

"For a Cyber Secured World."

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO) ON DEMAND |
DATA PROTECTION OFFICER (DPO) ON DEMAND |
CERTIFIED ETHICAL HACKER (C|EH) ON DEMAND |
CERTIFIED HACKER FORENSICS INVESTIGATOR (C|HFI) ON DEMAND

INTRODUCTION

Following the insights of CSX on the state of cybersecurity in 2019, there is an assumed skills gap in cybersecurity on most organizations. Almost 70% assume they are understaffed on cybersecurity. Almost 60% have open positions on cybersecurity. And almost one third of the inquiries assume they need at least 6 months to fill-in the vacancies. Also, they say one fourth of all the candidates, are underqualified for cybersecurity positions they offer. And still attacks continue to strive, and awareness isn't fostering. As such, 60% if information security professionals believe their company will be attacked this year, but 3 out of 4 inquired say cybercrime is under-reported, and half say its underreported even when its mandatory to report attacks to authorities. Only one third are highly confident about cybersecurity, although just 43% of all the companies inquired assume their cybersecurity report to a real CISO - Chief Information Security Officer.



And that's because most corporations decide not to hire a Chief Information Security Officer (CISO), or someone like champion their information security program, due to many factors, including cost and a lack of awareness of the importance of such a role. Typical companies have staff that manage their networks and servers, including firewalls or other security devices, but remain challenged when it comes to understanding their corporation's strategic security needs, as well as the path towards the security certifications needed to compete in the market. Employing an executive-level security professional can be very cost prohibitive and sometimes even overkill. Many organizations do not need a full-time CISO. All they really need is a trusted advisor who can provide thought leadership on creating an effective information security program and someone that can use the current resources in place to cost effectively manage the corporation's information security needs.

WHY SCORPIONSHIELD?

We are experienced professionals of cybersecurity and IT. Our work is mostly performed using manual testing approach, we do not only use automatic scanners but incorporate real attack techniques that could be used against an organization. Our reports are written by hand, not auto generated by tools. All our experience allows us to have a wider view on cybersecurity, we have knowledge from a technical perspective on how hackers operate and what are the biggest cybersecurity threats for today's world, but also from a management perspective from a CISO point-of-view and speak directly to company board members. We use knowledge with responsibility to help organizations protect themselves against online menaces.

SCORPIONSHIELD provides an On-Demand Service for Certified Chief Information Security Officers, Certified Ethical Hackers, Data Protection Officers, and Certified Hacker Forensic Investigators, and as such, assure an offering that provides companies with a recognized industry expert to take care of their security needs. Our services take the worry and confusion out of running a secure environment and dealing with complex regulatory compliance, leaving you free to run your business operations.

1. CERTIFIED CHIEF INFORMATION SECURITY OFFICER (C|CISO) ON DEMAND

The **C|CISO ON DEMAND** service works by allotting you a certain number of hours a week that an experienced consultant will use to help you build and manage your information security program. They will use the staff and resources you currently have available to ensure that both day-to-day security operations and tasks are carried out, as well as longer term security projects. On top of that, they will be available 24x7 to answer questions you may have or to respond to situations that may arise. Your assigned CISO, will totally manage the security of your environment leaving you the peace of mind to run your business. The **C|CISO ON DEMAND** completely believes in having an organized security program for any sized business. The first thing your CISO will do is to analyze the effectiveness of your current security program and, if necessary, make recommendations for improvements and then carry them out. If a security program is not in place, one will be created using **SCORPIONSHIELD** security's proprietary methodologies that are proven to provide world class security at the right level for your business. The security program is then managed and, as your business grows and develops, your CISO will be available for changes on security as necessary. A Corporate Security Assessment analyzes and discovers all the risks that pose a threat to your corporation. The threats that confront your business are constantly evolving and increasing in their complexity. Our consultants are skilled at analyzing corporate security programs to discover gaps, exploitable vulnerabilities and areas for improvement. Our consultants are able to offer concrete recommendations for accepting, reducing or transferring risk. The ultimate goal of our Corporate Security Assessment is to help identify the vulnerabilities that can put critical data at risk and cause downtime in your operations.

The **C|CISO ON DEMAND** can help you understand how to best protect your business:

- Discover where risks exist that may compromise your corporate assets
- Recommend cost-effective solutions to mitigate and prevent a breach in security
- Prioritize and set risk thresholds
- Assess your current security program
- Evaluate risk management tactics
- Move from a reactive security posture to a proactive one to prevent breach
- Demonstrate due diligence

The **C|CISO ON DEMAND** corporate security assessments helps businesses discover and evaluate technical, administrative and physical risks, and is tailored to meet each client's specific needs and may include:

- Vulnerability testing of your networks and systems
- System configuration reviews
- Network architecture reviews
- Reviews of policies and procedures
- Interviews with your key staff
- Physical security reviews
- Review of administrative security

C|CISO ON DEMAND helps businesses to identify and evaluate risk across the organization. To assist you to prioritize and deliver a business case for mitigation, a full report is provided detailing each vulnerability, its risk level, the business impact, customized recommendation and remediation effort. Meaningful metrics are also delivered that can provide added insight into the security readiness of your environment. These can be leveraged to give insight to management on the current state of security and can be utilized over a multi-year program to deliver cost justification for security expenditure.

2. DATA PROTECTION OFFICER (DPO) ON DEMAND

Regulatory compliance for information and network security is also known as IT Compliance. Securing the confidentiality, integrity and availability of your data is no longer just a security best practice; it is now a requirement for doing business. Whatever your size company or industry you are in, **DATA PROTECTION OFFICER (DPO) ON DEMAND** will check IT Compliance and can help you meet your regulatory and reporting requirements.

SCORPIONSHIELD security offers comprehensive IT security solutions across all aspects of compliance including; assessing, planning, implementing, monitoring, reporting and maintaining compliance. Our solutions for compliance are based on the latest standards and years of proven experience. They integrate comprehensive processes that are designed to encompass every aspect of security planning, management, and compliance reporting. The DPO implements and/or audits the ISO27001 ISMS (Information Security Management System) as he is responsible for protection data and privacy within each organization. Also, is responsible to delineate a path towards ISO27001 compliance and certification, from establishing the policies and procedures to engaging the implementation of the ISMS and executing it accordingly. It will help you build the system but also to organize it, control it and pass the necessary audits with the regulator towards certification. DPO will also help on compliance upon the GDPR General Data Protection Regulation, minding privacy of your customers and workers, to avoid unnecessary fines from being uncompliant, and meeting the necessary needs of your partners in business.

3. CERTIFIED ETHICAL HACKER (C|EH) ON DEMAND

The **CERTIFIED ETHICAL HACKER (C|EH) ON DEMAND** can help your business do the necessary Penetration Testing and Vulnerabilities Assessments.

A) VULNERABILITY ASSESSMENTS AND SECURITY AUDITS

SCORPIONSHIELD perform a broad scope of technical audits related to cybersecurity – security testing, vulnerability assessment, vulnerability scans, configuration audits and source code reviews. Vulnerabilities are continuing to evolve in complexity. Maintaining a secure environment in these conditions can be extremely difficult. These risks give security leadership serious concern as they question whether each and every vulnerability has been discovered and remediated.

Vulnerability Assessments helps businesses to identify and evaluate IT operational risks and internet security across the organization. To assist you to prioritize and deliver a business case for mitigation, a full report is provided detailing each vulnerability, its risk level, the business impact, customized recommendations and remediation effort. Meaningful metrics are also delivered that can provide added insight into the security and IT Security readiness of your environment. These can be leveraged to give insight to management on the current state of security and can be utilized over a multi-year program to deliver cost justification for security expenditure. Vulnerability Assessments may identify assets IT vulnerabilities with an in-depth customized assessment, enable businesses to prioritize vulnerability mitigation in order of the greatest threat to business assets based upon potential business impact, and enable businesses to build a business case to implement the appropriate mitigation and provide justification for security expenditure.

- **Cybersecurity audit**

  Security audits of IT systems are done to confirm, that the infrastructure deployed in the organization fulfils security requirements and does not contain security vulnerabilities compromising the confidentiality, integrity or availability.

- **Security config review, build review**

  Config reviews and build reviews are performed on software solutions such as operating systems, services (e.g. HTTP). We verify the configuration in relation to security based on benchmarks such as NIST, CIS and recommendations from the vendor.

- **Security code review**

  Source code audits may be connected with a whitebox pentest or be delivered as a separate service. The code is verified for security vulnerabilities. The analysis is performed manually with aid from automated tools and custom scripting. We have experience in reviewing applications written in i.e. Bash/C/C++/Java/JavaScript/.NET/PHP/Python/Ruby.

- **Vulnerability scans**

  Vulnerability scans are performed by automated tools, which identifies mostly already known security bugs, for which it has defined plugins. In the next phase identified vulnerabilities are manually verified by our pentesters in order to eliminate false positives.

- **IT security audit**

  When in need of conducting it security audit we recommend performing the following: config and build review, penetration testing and optionally code review. Security audits of IT systems are done to confirm, that the infrastructure deployed in the organization fulfils security requirements.

B) PENETRATION TESTING

Penetration Testing assists businesses to safely identify vulnerabilities before attackers exploit them. Penetration Testing assists organizations to assess the security posture of their networks, buildings and staff by safely identifying technical, physical and administrative vulnerabilities before they are attacked. Our highly skilled security consultants use real-world scenarios to demonstrate how attackers can gain access to sensitive data, buildings or systems and lead to significant loss to your business. Our IT Consultants can perform penetration testing to secure your network security and data. With the proper IT service, IT support and IT consulting **SCORPIONSHIELD** can protect you, from a hack or cyber-attack.

During penetration testing, our security consultants will conduct covert activities typical of an attacker attempts to compromise servers, buildings and sensitive information. The testing is conducted in a safe and controlled exercise that is completely pre-authorized by you before an un-authorized attacker gets into your buildings and servers, causing you great loss. A penetration can be likened to surveying a rabbit proof fence, which must be whole to keep the rabbits out. In surveying the fence, the penetration tester may identify a single hole large enough for a rabbit (or themselves) to move through, once the defense is passed, any further review of that defense may not occur as the penetration tester moves on to the next security control. This means there may be several holes or vulnerabilities in the first line of defense and the penetration tester only identified the first one found as it was a successful exploit. This is where the difference lies between a vulnerability assessment and penetration test - the vulnerability assessment is everything that you may be susceptible to, the penetration test is based on if your defense can be defeated.

SCORPIONSHIELD Penetration Testing services can or may include:

- **Technical testing (*)** on Internet based servers and internal networks, Wireless/3G/4G/5G networks
- **Social Engineering** telephone calls and War dialing to test the security awareness of your employees
- **Phishing and Spear Phishing** Emails to your employees to test their security awareness
- **Physical Security** testing (Black Ops teams available upon request)
- **Physical Assessment** of sensitive information unprotected within the building

You can choose all these options for a full and comprehensive test or choose just a few to in a specific area you would like tested. At the end of the test, you will receive a detailed, professional report of the findings split into two sections; an executive summary and also a detailed technical report. The report will detail what testing was carried out and provide a clear table that will explain each finding, its business impact and remediation recommendation. This can be used as a road map of what to prioritize in IT security initiatives and spending.

Technical testing (*) is conducted to verify security of a targeted asset such as network, web, mobile or client-server application, and may include:

- **Cybersecurity testing**

  It is one of our core services, we have many years of experience in performing penetration testing and until now we have delivered several hundred tests to our customers. All pen testers performing testing hold multiple certificates e.g. OSCP (Offensive Security Certified Professional) and have a proven track record in the industry. We fulfill the formal requirements often required by customers in terms of delivering a penetration test such as PCI DSS Penetration Testing Guidance. All reports are written by our consultants and not thoughtlessly generated by automatic security scanners. Additionally, our pen testers have identified many vulnerabilities in popular software and successfully participated in bug bounty programs.

- **Black box penetration testing**

Both infrastructure and application pen testing can be performed from a outside attacker perspective meaning that the tester does not hold any knowledge regarding the targeted system apart from those available publicly. No information about the architecture and customer systems is delivered, no user accounts except those that can be created by an attacker (e.g. by registering in the application). Usually when conducting a security audit of a web application we use a gray box approach, which gives us some information about the audited system (e.g. documentation, description of the system functionalities) and accounts for each role in the systems are delivered, so we are able to check both vertical and horizontal privilege escalation, meaning accessing data and/or functionalities of higher privileged user and a different user with similar access rights.

- **White box penetration testing**

This type of a security audit is an extended version of gray box pen testing in which testers have full knowledge of the targeted asset. In case of a web application we are given access to both documentation and the source code additionally to what is granted in a gray box test.

- **Web application penetration testing**

We deliver web application penetration testing in accordance with popular and widely accepted OWASP methodology (The Open Web Application Security Project), including OWASP Top 10 and OWASP ASVS (Application Security Verification Standard) extended by our experience. We do not limit ourselves only to OWASP listed vulnerabilities and aim to find also business specific vulnerabilities that can pose a real threat to the business of the customer and which are often missed by automated vulnerability scanners.

- **Software penetration testing**

We deliver desktop application penetration testing and client-server application penetration testing. We can cover security testing of applications written in C/C++/C# and Java for Windows, Linux and OS X platforms.

- **Mobile application penetration testing**

We perform mobile application penetration testing for iOS and Android platforms. We base our methodology on OWASP Mobile (The Open Web Application Security Project), including OWASP Mobile Top 10 and OWASP MASVS (Mobile Application Security Verification Standard) enhanced by our own experience in identifying vulnerabilities in mobile application.

- **Infrastructure penetration testing**

We perform penetration testing of network infrastructure (LAN/WAN/WLAN), according to the PTES framework (The Penetration Testing Execution Standard). Tests can be conducted from both external (Internet, Wi-Fi etc.) and internal (LAN, VPN) networks.

- **LAN Network penetration testing**

Security audit of a local network can be performed locally on premises or via VPN. The difference compared to infrastructure pen testing is that the pen tester is given access on the level as if the intruder already gain access to the company internal network or it simulates a rogue employee trying to do harm from the inside.

- **WiFi penetration testing**

WiFi penetration testing aims to test the security of locally deployed wireless networks. It aims either to break into a protected WiFi network as well as privilege escalation from a guest network and attacking the users. Wireless security is also a part of our Red Team services which aims to perform social engineering attacks against unsuspecting WiFi users, for example by running a rogue AP (Access Point).

C) RED TEAM AND BLUE TEAM OPERATIONS

Red Team operations are authorized attacks reflecting real capabilities of adversaries. Red Team covers various aspects such as network, social engineering and physical security.

- **Adversary simulation**

  Thanks to our vast knowledge in the cybersecurity field we are able to deliver high quality simulated APT (Advanced Persistent Threat) attacks meaning CPH (Cyber-Physical-Human) Red Team operations are meant to reflect real cyber-attack scenarios, which might be aimed at a specific organization. Red Team exercises are used to assess the current state of security in a targeted company, employees' awareness, as well as the reaction time of internal security teams such as SOC (Security Operations Center).

- **Social engineering**

  We perform authorized social engineering attacks, which usually refers to preparing and delivering phishing campaigns targeting customer employees. The goal is decided individually with each customer, for example it can be credential harvesting, using them for further escalation and simulating a real attack by trying to exfiltrate data outside the organization. In a more basic version, it can simply be gathering statistics of the campaign success ratio (number of clicks, gathered credentials).Other scenario may be aimed at WiFi users, where our consultants set up a rogue AP (Access Point) posing as the legitimate one. When the user connects, we may try to perform MiTM (Man-in-The-Middle attacks) meaning capturing sensitive data, planting specially crafted executables by hijacking downloaded files in order to gain further access.

- **Red Team vs Penetration Testing**

  Red Team differs from penetration testing on multiple levels:

  - it is not limited by a very strict scope (pen testers limited to gain access to specific web application),
  - it is not about finding as many security vulnerabilities as possible, but finding the most effective way to break into to organization or achieve a specific goal (e.g. steal sensitive data),
  - it is not limited only to technology, it includes human factors (social engineering), as well as physical security (e.g. on premises access controls),
  - it cannot be too noisy, as it often aims to demonstrate bypassing of additional security controls and test the effectiveness of the internal security teams.

- **Network attacks**

  As a part of Red Team operations, we conduct network attacks both external and internal, where the main goal is gaining access to important company resources' data or as a way to get inside the internal network. However, for the most part it is used for escalation after gaining initial access to the network using social engineering or physical access.

- **Physical security**

  Main goal of physical security testing in case of Red Team is gaining access to the organization building, restricted access zones, documents, company devices and the internal network.

D) THREAT HUNTING AND INTELLIGENCE

Our unique approach stands out with the fact that we are not only base our detection on known active crime groups but focus on a wider perspective which allows us for more effective detection of targeted attacks, which are not detected by common tools and security software. Threat hunting means an active search for intruders in the organization infrastructure, sort of proactive digital forensics helping to increase detection capabilities of both inside and outside threats. We offer threat hunting services in both offense and defense.

- **Blue Team & Blue Teaming**

Threat hunting is a constantly evolving process not a technology. We have a solid knowledge on real attacks and track covering techniques which comes directly from the services we offer – **SCORPIONSHIELD**, penetration testing, as well as analysis and detection of such attacks – digital forensics and incident response. We dissect the attacker's methods in order to detect them independently of which tools were used to perform them, simultaneously decreasing the number of operations on analyzed data that needs to be performed by the detection system resulting in increasing the efficiency. Additionally, we use so called data enrichment for supporting internal data such as logs with outside information from our proprietary CTI (Cyber Threat Intelligence) system.

- **Proactive threat discovery**

We know how to effectively identify attack symptoms and intruder presence in the organization infrastructure. A sample task for a threat hunter is to run a dedicated software (e.g. a honeypot) or monitor the DNS traffic inside a network looking for potentially malicious activity by e.g. checking entropy, types of DNS requests, comparison of domains with IOC (Indicator of Compromise) received from threat intelligence etc. On the other hand, log analysis in this case is not only limited to monitoring base events but means deep analysis by connecting many sources which can indicate that integrity has been compromised. Every solution is individually prepared to fit the customer needs in order to get best detection rates. Thanks to that type of approach there is a real possibility of detecting an attack, including the targeted ones which can help in reacting on time before real damage is done.

- **Threat Intelligence**

Cyber Threat Intelligence (CTI) is used to get constant information updates from outside source about a given organization. The services consist of two main parts: information for security teams, mostly used to automatic data enrichment for internal monitoring SIEM systems, IPS (Intrusion Prevention System) or IDS/NIDS/HIDS (Intrusion Detection System, Network, Host). Simplest example of such enrichment might be acquiring IP addresses information from the honeypot network used by attackers or detecting changes of open ports in the company infrastructure. We use a dedicated proprietary software, which depending on customer needs automatically looks for potential threats or changes that might indicate a compromise. We support infrastructure monitoring with data from CTI which allows us to effectively detect targeted attacks. Our software collects information available on the Internet (OSINT) and actively monitors organization assets to look for changes inside both external (WAN) and internal (LAN) networks.

- **OSINT**

We perform OSINT engagements (Open-Source Intelligence) where we gather significant amount of information about the target organization on the Internet.

- **SIEM rules**

We create rules for SIEM (Security Information and Event Management) systems. It is a part of our threat hunting service, like with extending logging capabilities, honeypot construction etc.

- **Security Operations Center (SOC) and SOC3 service**

Threat hunting service is usually delivered as the 3rd, last line in the Security Operations Center (SOC). Additionally, with our customer or partner we are able to offer full SOC outsourcing, consisting of 3 lines, working 24/7. We provide the last line of Security Operations Center (SOC). It can be offered directly to the customer, which only has 1st and 2nd line of support. Alternatively, we offer this service as a partnership, for of support and in need of professional threat hunting and incident response.

4. CERTIFIED HACKER FORENSICS INVESTIGATOR (C|HFI) ON DEMAND

The **CERTIFIED HACKER FORENSICS INVESTIGATOR (C|HFI) ON DEMAND** is a Digital Forensics Investigator and Incident Response Specialist, which covers topics such as collecting and securing digital evidence, performing analysis after breaches and recovering deleted data.

- **Computer Forensics**

  We offer expert services in computer forensics especially related to cybersecurity meaning DFIR (Digital Forensics and Incident Response). We have a status of IT Expert Witness in Portugal and have taken part in securing evidence on crime scenes. We use highly specialized equipment and commercial tools to perform our forensics analysis.

- **Incident response (CERT, CSIRT)**

  As a CERT (Computer Emergency Response Team) known also as a CSIRT (Computer Security Incident Response Team) we can help in situations when a security incident already has taken place. We will advise how to approach the problem and get expected results and perform a reliable analysis of the event. Our team will deliver a complex service starting from properly securing the data to analysis and delivering the final report with the findings. In order to help the customers securing the data properly on their own we offer a know-how on how to do it for Windows and Linux systems.

- **Incident analysis**

  We analyze IT systems after they have been breached (hacked). We will help to secure the evidence, determine how the attack occurred, what operations have been performed by the attackers.

- **Log, disk, RAM and network analysis**

  We perform all sort of analysis on hard disks, logs (events), RAM memory dumps and network traffic.

- **Secure data erasing**

  In case a customer's wants to securely remove sensitive data out of a undamaged hard disk we are able to help. This service may be used in cases such as old storage being decommissioned and later set up for sell or before returning a rented equipment. After the process no one will be able to recover data from the disk even with the help of digital forensics tools.

- **Practical computer forensics analysis**

  This cover securing digital evidence, hacker attack analysis, backdoor and rootkit detection.

- **Corporate espionage**

  We help customers in detecting acts of corporate espionage in cases of suspicion where competition or rogue employees are trying to obtain the company secrets.

- **Malware analysis**

  We perform malware analysis, both behavioral and static analyses approaches are used by our analysts. Also, we are able to analyses disks for malware presence and identify it.

5. QUALITY, PARTNERSHIP, CONFIDENCIALITY AND ACADEMY OF EXPERTS

QUALITY

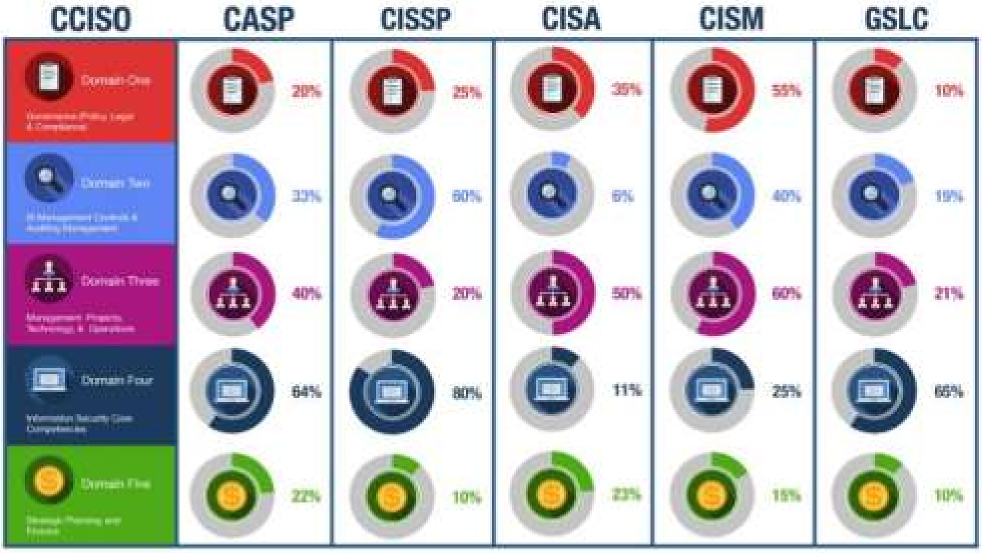
We only employ leading industry experts with extensive testing experience. All our consultants have at least 10 years' experience and have the well-recognized security certification:

- Certified Chief Information Security Officers - C|CISO by ECCOUCIL ™
- Certified Ethical Hacker – C|EH by ECCOUCIL ™
- Certified Hacker Forensics Investigator – C|HFI by ECCOUCIL ™
- Certified Information Privacy Manager - CIPM IAPP ™ International Association for Privacy Professionals
- ISO27001 Lead Implementer & Lead Auditor and GDPR Expert by BSI ™ - British Standards Institute

PARTNERSHIP

SCORPIONSHIELD is using the certified knowledge on information security from the most reputed information security training institution of the world, the **EC-COUNCIL ™** – a renowned world leader in Information Security Training and Certification (credited by ANSI, Committee on National Security Systems – CNSS, National Security Agency – NSA, the Department of Defense – DoD, CREST Equivalency, and Department of Veterans Affairs.

Our experience also found the in-depth and broadening of EC-COUNCIL courses to surpass most of the others, and that's why we are fostering and striving on our partnership relation with them.



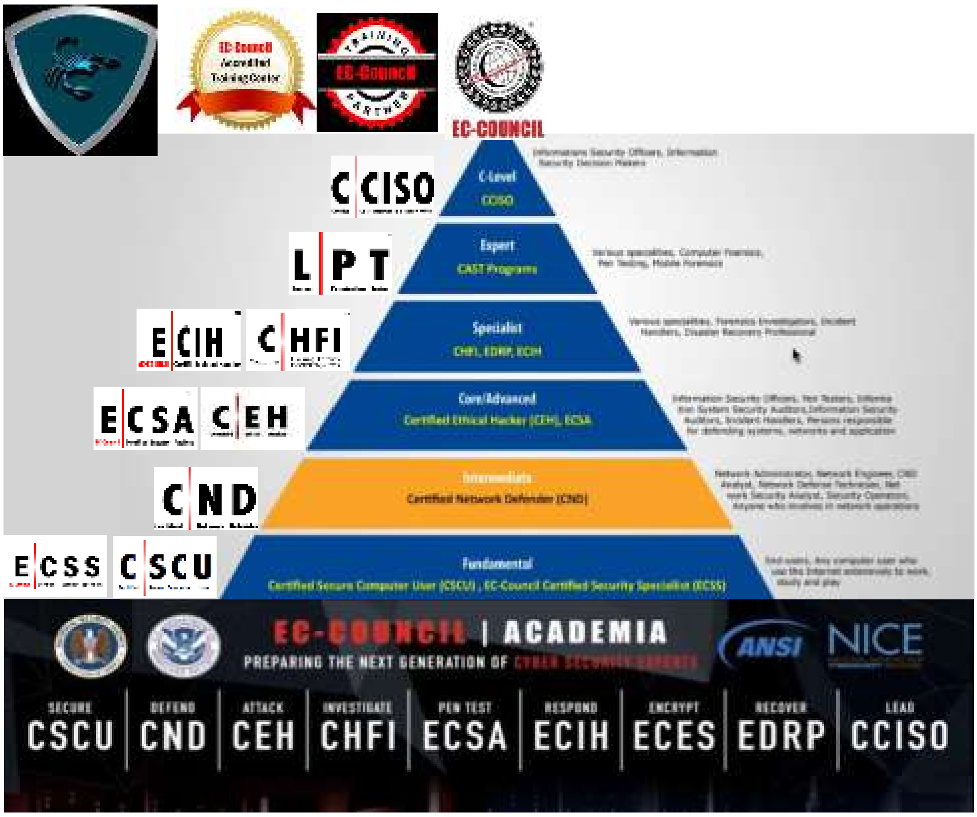
Our consultants conduct safe, high quality technical testing and use only manual penetration techniques. Our technical testing is not a mere security scan of your network. All technical testing is manually carried out according to the industries best practices. Our consultants are also experts at building infiltration and able to demonstrate how buildings can be infiltrated by an attacker and offer clients recommendation for improving physical security.

CONFIDENCIALITY

Within every Project, Corporate or Technical Assessment, or Testing, **SCORPIONSHIELD** and its consultants will provide a Non-Disclosure Agreement (NDA) to attain full confidentiality of the service.

ACADEMY

SCORPIONSHIELD trains its own consultants, in accordance with our partnership with EC-COUNCIL, to excel the necessary expertise for our projects. We build our own academy, through EC-COUNCIL approved courses, with levels of expertise and leadership, to provide the best service. This ethical hacking training will immerse the participants into an interactive environment where they will be shown how to scan, test, hack and secure their own systems. The lab's intensive environment gives each participant in-depth knowledge and practical experience with the current essential security systems. Participants will begin by understanding how perimeter defenses work and then will be led into scanning and attacking their own networks (no real network is harmed). During this ethical hacking course, students learn how intruders escalate privileges and what steps can be taken to secure a system. At the end, they can candidate for exam and earning a Certificate.


EC-Council Accredited Training Center
TRAINING EC-COUNCIL PARTNER
EC-COUNCIL
CCISO
LPT
ECIH
CHFI
ECSA
CEH
CND
ECSS
CSCU
C-Level
CCISO
Informations Security Officers, Information Security Decision Makers
Expert
CAST Programs
Various specialties, Computer Forensics, Pen Testing, Mobile Forensics
Specialist
CHFI, EDRP, ECIH
Various specialties, Forensics Investigators, Incident Handlers, Disaster Recovery Professional
Core/Advanced
Certified Ethical Hacker (CEH), ECSA
Information Security Officers, Pen Testers, Information System Security Auditors, Information Security Auditors, Incident Handlers, Persons responsible for defending systems, networks and application
Intermediate
Certified Network Defender (CND)
Network Administrator, Network Engineer, CND Analyst, Network Defense Technician, Network Security Analyst, Security Operators, Anyone who involves in network operations
Fundamental
Certified Secure Computer User (CSCU) , EC-Council Certified Security Specialist (ECSS)
End users, Any computer user who use the Internet extensively to work, study and play
EC-COUNCIL | ACADEMIA
PREPARING THE NEXT GENERATION OF CYBER SECURITY EXPERTS
ANSI
NICE
SECURE CSCU
DEFEND CND
ATTACK CEH
INVESTIGATE CHFI
PEN TEST ECSA
RESPOND ECIH
ENCRYPT ECES
RECOVER EDRP
LEAD CCISO

In the hierarchy, the fundamentals reside on the understanding through CSCU (Certified Secure Computer User) and ECSS (Certified Security Specialist). Further going above the hierarchy, at Intermediate Level, we have the CND (Certified Network Defender). Whereas the most advanced certifications on the Core Level, are CEH (Certified Ethical Hacker) and ECSA (EC-COUNCIL Certified Security Analyst), that sets the baseline for any security professional. A Specialist is the next and last level of technical expertise, where reside the CHFI (Certified Hacking Forensics Investigator), the ECIH (EC-COUNCIL Certified Incident Handler) and finally the EDRP (EC-COUNCIL Disaster Recovery Professional). The C-level executive course is CCISO (Certified Chief Information Security Officer) which is the most distinguish competence of a Security Professional.