Security & Defense Division Profile & Offered Cybersecurity Services

CYBER ZONES is a leading cybersecurity consulting firm dedicated to serving organizations across the Middle East, we focus on delivering sound, sensible and well-structured cyber security services and directions aligned to business objectives.

Mission

At CYBER ZONES we are dedicated in protecting our customers from cyber-attacks and comply with national and international cyber security standards.

Vision

At CYBER ZONES we provide innovative services in the cybersecurity landscape. Our team of experts combines creativity and technology to help businesses thrive online.

CYBER ZONES
Cyber Security Services

CYBER ZONES CORE VALUES

Respect	Precise	Honesty
Quality	Customer Satisfaction	Enablement

Cyber Zones Consultants

Our certified consultants have diverse experience from international firms and conducted countless cyber security engagements with high end customers

CYBER ZONES OPERATIONS PHASES

Identify & Analyze Phase

Connect with the customer to identify the needs and recommended cyber security services.

Collect & Plan Phase

Collect required information and properly plan the engagement.

Recommend & Deliver

Recommend professional services and products and smartly deliver them based on a clear action plan.

CYBER ZONES is a leading cybersecurity provider catering to a wide range of industries with customized solutions designed to tackle the unique security challenges of today's digital landscape. Through our specialized **Security & Defense Division - SDD**, we deploy dedicated **units** that operate based on the principles of separation of duties, need-to-know approach, layered security, and defense-in-depth strategies. This structured framework ensures comprehensive, multi-layered protection, enhancing resilience against evolving cyber threats.

Security & Defense Division

- GOVERNANCE, RISK MANAGEMENT & COMPLIANCE | GRC UNIT
- CYBER ADVISORY UNIT
- CYBER INVESTIGATION UNIT
- IOT SECURITY UNIT
- TRAINING SERVICE UNIT

AT A GLANCE | CYBER ZONES ADVANCED CYBERSECURITY SERVICES

5 specialized units to deliver the best Cybersecurity services to our clients

CYBER ZONES
Cyber Security Services

WE DON'T JUST HELP YOU MEET STANDARDS. WE HELP YOU LEAD WITH CONFIDENCE.

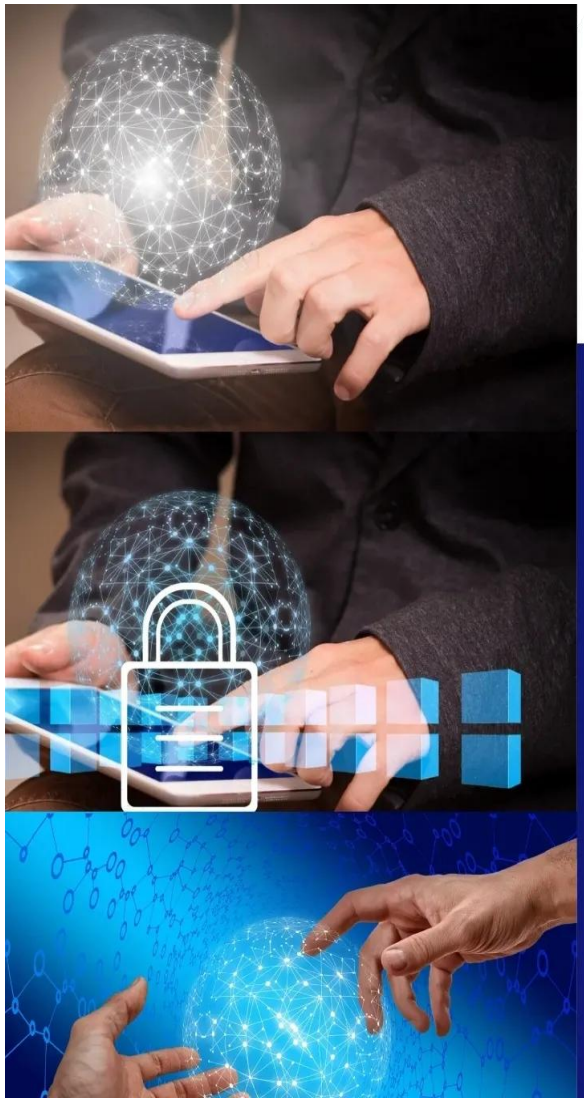
GRC UNIT

CYBER ZONES

In today's rapidly evolving regulatory landscape, businesses face increasing pressure to stay compliant, secure, and resilient. At CYBER ZONES our **Governance, Risk, and Compliance (GRC) Unit** is your trusted partner in navigating this complex terrain. With a team of seasoned professionals and a deep understanding of international and national regulatory frameworks, we empower organizations to align business objectives with cybersecurity and compliance requirements, seamlessly and effectively.

We don't just help you meet standards, our GRC unit help you lead with confidence.

CYBER ZONES
Cyber Security Services



GRC UNIT
CYBER ZONES

Whether you're looking to meet national mandates, prepare for audits, or elevate your security posture, we're here to guide your journey.

Our GRC Unit is committed to **enabling businesses to operate securely, transparently, and in full compliance** with relevant laws, regulations, and best practices, we aim to:

- **Reduce risk exposure** through proactive governance
- **Ensure full regulatory compliance** across your operations
- **Build resilient frameworks** that adapt to change and support sustainable growth
- **Enhance executive decision-making** through actionable insights and reporting

NCA Controls P-D-C-A Service

Stay ahead of Saudi Arabia's regulatory mandates with expert guidance across all NCA frameworks:

- Essential Cybersecurity Controls (ECC)
- Cloud Cybersecurity Controls (CCC)
- Critical Systems Cybersecurity Controls (CSCC)
- Data Cybersecurity Controls (DCC)
- Telework Cybersecurity Controls (TCC)
- Operational Technology Cybersecurity Controls (OTCC)

SAMA Assessment Service

Ensure compliance with the Saudi Arabian Monetary Authority's cybersecurity requirements, Cyber Zones specialized in the following SAMA frameworks:

1- SAMA CSF
2- SAMA ITGF
3- SAMA BCMF
4- SAMA ORMF
5- SAMA TPRM
6- SAMA Data Governance Framework
7- SAMA Open Banking Framework
8- SAMA Fintech Regulatory Sandbox
9- SAMA Cloud Computing Regulatory Framework

ISO/IEC 27001 – Information Security Management System (ISMS)

From design to certification, we help build ISMS aligned with ISO 27001, ensuring a secure and auditable environment.

ISO/IEC 27701 – Privacy Information Management System (PIMS)

Enhance your data privacy program and ensure compliance with global privacy laws like GDPR and national regulations through ISO 27701 implementation.

PDPL Readiness Assessment

The **PDPL (Personal Data Protection Law) Readiness Assessment Service** by Cyber Zones helps organizations evaluate their current state of compliance with Saudi Arabia's Personal Data Protection Law (PDPL). This service identifies gaps and areas for improvement in privacy governance, data handling processes, security controls, and legal obligations to ensure readiness for regulatory compliance.

Data Mapping & Records of Processing Activities (RoPA)

The **Data Mapping & Records of Processing Activities (RoPA) Service** by Cyber Zones assists organizations in systematically identifying, documenting, and managing all personal data processing activities in alignment with data protection regulations such as PDPL, GDPR, and ISO/IEC 27701.

Privacy Impact Assessments (PIAs / DPIAs)

The **Privacy Impact Assessment (PIA) / Data Protection Impact Assessment (DPIA) Service** offered by Cyber Zones supports organizations in identifying, assessing, and mitigating privacy risks associated with processing personal data, in alignment with global privacy laws such as PDPL, GDPR, and ISO/IEC 27701 requirements.

Third-Party Data Processing Compliance

The **Third-Party Data Processing Compliance Service** by Cyber Zones assists organizations in evaluating and managing the privacy and security risks associated with third-party vendors and service providers that process personal data on their behalf. This service ensures compliance with regulations such as PDPL, GDPR, and ISO/IEC 27701 by verifying that third parties meet contractual, legal, and technical requirements for data protection.

Data Protection and Privacy Program Development

Build a privacy first culture and meet local and international data protection requirements through:

- Data classification and mapping
- Consent and rights management frameworks
- Privacy policies and procedures
- DPIAs (Data Protection Impact Assessments)

Risk Management Service

The **Risk Management Service** offered by Cyber Zones is designed to help organizations identify, assess, prioritize, and mitigate cybersecurity and privacy risks in alignment with industry best practices and regulatory requirements such as ISO 31000, NIST, PDPL, and SAMA frameworks.

GAP Assessment Service

The **Gap Assessment Service** by Cyber Zones provides a focused evaluation that compares your organization's current security posture against a selected cybersecurity framework or standard. This service identifies gaps and areas needing improvement, enabling targeted remediation efforts to enhance overall security and compliance. Our experts are specialized in the following assessments: ISO 27001, ISO 22301, NIST CSF, PCI DSS, GDPR, BCM, PDPL, KSA-NCA, SAMA CSF, ITGF, BCM & Cryptography assessment

Regulatory Gap Assessments & Remediation Planning

The **Regulatory Gap Assessments & Remediation Planning Service** by Cyber Zones assists organizations in evaluating their compliance status against applicable laws, regulations, and industry standards, identifying gaps that could expose them to legal or operational risks. This service is designed to provide clear insights into areas of non-compliance and develop strategic remediation plans to achieve regulatory adherence.

Policy & Procedure Development and Governance

We create, review, and manage your organization's cybersecurity, privacy, and risk policies. Typical documents include:

- Acceptable Use Policies (AUP)
- Data Protection Policies
- Access Control Policies
- Incident Response Plans
- Information Classification Policies
- Security Awareness and Training Policies

Internal Audit & Compliance Monitoring

The **Internal Audit & Compliance Monitoring Service** offered by Cyber Zones is designed to help organizations systematically evaluate the effectiveness of their cybersecurity and privacy controls, ensuring ongoing adherence to applicable standards, regulations, and internal policies.

Cybersecurity Governance Program Development

The **Cybersecurity Governance Program Development Service** by Cyber Zones helps organizations design and implement a robust cybersecurity governance framework that aligns with business objectives, regulatory requirements, and industry best practices.

ISO/IEC 42001 – Artificial Intelligence Management System (AIMS)

The **ISO/IEC 42001 – Artificial Intelligence Management System (AIMS) Service** provided by Cyber Zones assists organizations in establishing, implementing, and maintaining an AI management system aligned with the ISO/IEC 42001 international standard. This service ensures responsible, ethical, and secure use of artificial intelligence technologies within the organization.

Business Continuity Management (BCM) Assessment

The **Business Continuity Management (BCM) Assessment Service** by Cyber Zones evaluates your organization's capability to maintain critical business functions during and after disruptive events. This service helps organizations align their continuity and resilience planning with internationally recognized standards such as ISO 22301 Business Continuity Management System (BCMS) and regulatory frameworks like SAMA BCM requirements.

Personal Data Protection Law (PDPL) Compliance

The **Personal Data Protection Law (PDPL) Compliance Service** offered by Cyber Zones supports organizations in achieving and maintaining compliance with the Saudi Arabian PDPL requirements. This service helps organizations establish a comprehensive privacy program aligned with PDPL mandates, ensuring lawful, fair, and transparent processing of personal data.

Cybersecurity Operational Technology (OT) Assessment

The **Cybersecurity Operational Technology (OT) Assessment Service** provided by Cyber Zones is designed to evaluate the security posture of your organization's OT environments, including industrial control systems (ICS), SCADA, and other critical infrastructure components.

Regulatory Compliance Monitoring-as-a-Service (RCMaaS)

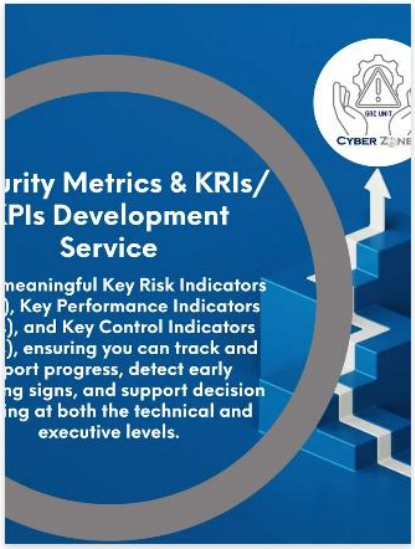
The **Regulatory Compliance Monitoring-as-a-Service (RCMaaS)** by **Cyber Zones** provides organizations with ongoing, expert-driven oversight of their cybersecurity, privacy, and IT governance compliance posture.

Data Classification & Handling Program

The **Data Classification & Handling Program** by **Cyber Zones** helps organizations design, implement, and enforce a structured framework for classifying and managing data based on its sensitivity, business value, and regulatory obligations.

Records Management & Retention Compliance

The **Records Management & Retention Compliance Service** by **Cyber Zones** is designed to help organizations establish, audit, and optimize their practices for managing records and information throughout their lifecycle ensuring compliance with regulatory, legal, and business requirements.



Security Metrics & KRIs/KPIs Development

The **Security Metrics & KRIs/KPIs Development Service** by **Cyber Zones** helps organizations define, implement, and operationalize a structured measurement framework to monitor the performance, effectiveness, and risk posture of their cybersecurity and GRC programs.

Regulatory Intelligence & Advisory Services

The **Regulatory Intelligence & Advisory Services** by **Cyber Zones** are designed to help organizations continuously monitor, interpret, and respond to evolving cybersecurity, privacy, and IT regulations that impact their business operations locally and internationally.

Quantum Risk Assessment Service

Quantum Risk Assessment service offered by Cyber Zones aims to proactively evaluate and understand the exposure of clients' digital environments to the emerging risks posed by quantum computing, particularly its potential to break current cryptographic algorithms.

Quantum Readiness Advisory Service

Quantum Readiness Advisory service provides strategic guidance and maturity assessment for organizations preparing to transition into the post-quantum era. The service evaluates the organization's readiness in terms of people, processes, and technologies to adopt quantum-resilient cryptography and practices.

Post-Quantum Cryptography (PQC) Transition Support

Post-Quantum Cryptography Transition Support is a hands-on service that helps organizations migrate from classical cryptographic algorithms (such as RSA and ECC) to quantum-resilient alternatives approved or shortlisted by NIST.

CYBER ZONES
Cyber Security Services

SECURITY IS FELXIBILITY NOT COMPLEXITY

Unless you are solely responsible for staying on top of cyber security, it is almost impossible to keep up with all the trends. This is why cyber advisory is in such high demand. Companies of all sizes often need professional second-options and opinion, based on global cyber insights and subject-matter expertise.

CYBER ADVISORY UNIT GOALS

Cyber Advisory unit aims to articulating your company's cyber security problems and needs, offering and assessing solutions and services, and then suggesting an implementation short- and long-term roadmap for the best plans based in NIST framework.

CYBER ADVISORY UNIT SERVICES

CYBER ZONES
Cyber Security Services

Cybersecurity Inspection Service

Seeks to pinpoint vulnerabilities in both internal and external assets of clients, enabling our cybersecurity consultants to gain a comprehensive understanding of the protection levels and potential attack surfaces related to our clients' assets in a practical way. This assessment helps to outline a strategic roadmap for both immediate and future actions that clients can take.

Low Level Architecture Auditing Service

Low Level Architecture auditing aims to gather detailed information regarding each OS, network and security device and recommend the best actions to take to reach optimal security performance level, this service is a detailed configuration review

Vulnerability Scanning Service

Using automated tools, a report that contains threats and vulnerabilities will be provided to client along with remedy actions to take.

Vulnerability Assessment Service

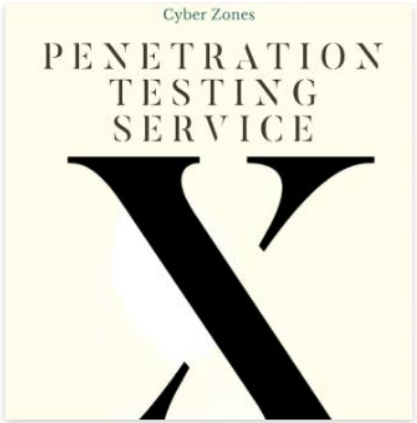
Aims for identifying vulnerabilities and **highlight the criticality** of detected vulnerabilities on a system without exploiting them.

CYBER ADVISORY UNIT SERVICES

CYBER ZONES
Cyber Security Services

Vulnerability Management Service

We will manage, and controls threats related to your operations by identifying, assessing, prioritizing and responding to potential vulnerabilities



Penetration Testing Service

We perform Penetration Testing using manual methods to systematically compromise servers, endpoints, web applications, Mobile applications, wireless networks, network devices and other potential points of exposure.

Cybersecurity Consultation Service

Cyber Security Consulting with an experienced security professional provides unparalleled peace of mind. Vulnerabilities can be identified and risks appropriately prioritized. Your security stance can be greatly improved. Your team can even be taught how to maintain your improved security configuration going forward.

Security Awareness Newsletter

We will develop a unique set of security awareness newsletters with catchy images and unique slogans which will attract the attention of end users and assist in establishing a proper security environment within the organization, this service focus on develops a sense about the important on security and complying with security standard and procedures.

CYBER ADVISORY UNIT SERVICES

CYBER ZONES
Cyber Security Services

Social Engineering Service | Phishing

You can test and educate your employees on how to spot phishing and avoid attacks. Find out what could happen to your organization before the bad guys try.

Social Engineering Service | Vishing

Vishing simulation is a method of trying to gather statistical information using deceptive phone calls and voice messages.

RED Team Service

specialized cybersecurity service where ethical hackers simulate real-world cyberattacks to test your organization's security defenses. The goal is to identify vulnerabilities, assess detection and response capabilities, and improve overall security posture.

vISO & vCISO Services

vISO & vCISO provides access to seasoned experts with over 20 years of experience in information and cybersecurity.

CYBER ADVISORY UNIT SERVICES

CYBER ZONES
Cyber Security Services

White Team Service

Oversees, documents, and evaluates the any security exercise running by your security team, this service aims to monitors, records actions, and ensures adherence to rules and provide **recommendations** for security enhancements and future training.

Black Team Service

Focuses on **real-world resilience testing** by assessing your organization's security **without prior knowledge** or coordination with internal security teams. **Our black team** operate in a way that closely mimics how actual adversaries would target your organization by testing **technical, physical, and human security** without prior warning.

Gold Team Service

Simulated theoretical tabletop crisis simulation (aka War Room Simulation)

Segmentation Test Service

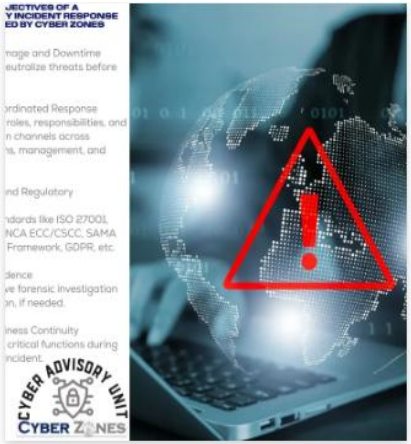
Crucial service that ensures network segmentation controls are effectively **restricting access and preventing unauthorized lateral movement** within your organization's infrastructure. It helps verify whether attackers or malware can move between different zones, such as IT, OT and cloud environments (CSP and CST).

CYBER ADVISORY UNIT SERVICES

CYBER ZONES
Cyber Security Services

Stress Testing Service

is a specific service that helps your organization understand just how well you are prepared for the different DOS attack vectors that. The service consists of simulations of high load on systems and are carried out in a strictly controlled and pre-scheduled manner.

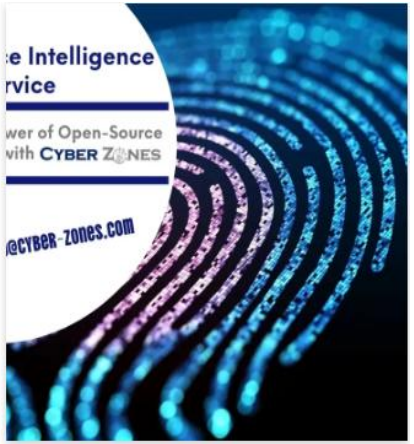


Cyber Incident Response Plan

The purpose of this service is to provide operational structure, processes and procedures tailored to our clients, so that they can effectively respond to incidents that may impact the function and security of digital assets, information resources, and business operations.

Dark Web Monitoring Service

Dark Web Monitoring Service aims to helps critical employees and organizations monitor and track illicit or unauthorized activity related to their sensitive information on the **dark web**.



Open-Source Intelligence Service

OSINT Service utilizes publicly available data and information to identify potential security risks. Our OSINT (Open-Source Intelligence) team works diligently to detect any misuse of sensitive information, ensuring the confidentiality and integrity of your company's operations and protecting your employees from compromising actions.

CYBER ADVISORY UNIT SERVICES

CYBER ZONES
Cyber Security Services

Ransomware Readiness Assessment service

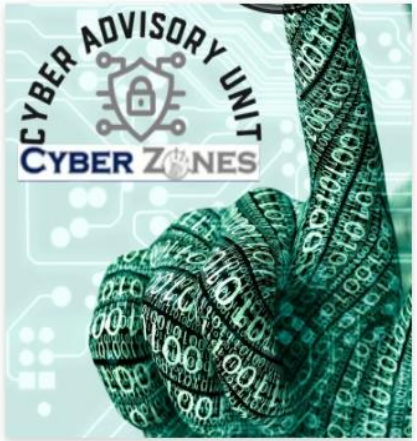
is a part of cyber risk management service which aims in defending against ransomware attacks, Ransomware Readiness Assessment service focuses on preparing you to better prevent, detect, respond and recover from ransomware.

Minimum Baseline Service

Minimum Baseline Security (MBS) defines the essential security controls and configurations every system, device, and application must implement to ensure a consistent and secure operating environment across the organization.

Source Code Review

Source Code Review is a security assessment service that analyzes application source code to identify vulnerabilities, logic flaws, and insecure coding practices before deployment—ensuring your software is secure by design.



MDR Consultation Service

Cyber Zones offers a cybersecurity advisory service that helps organizations plan, implement, or optimize their **Managed Detection and Response (MDR)** capabilities. Unlike the MDR service itself (which actively monitors and responds to threats), the **consultation service** focuses on strategic guidance, technical assessment, and solution alignment.

MDR Consultation Service includes

- SIEM
- Threat Intel
- Threat Hunting
- Malware Analysis
- EDR
- Integration & Optimization
- Playbooks
- Brand Protection
- IHR
- UBA
- Deployment Guidance
- Use Case Design & Automation
- IR Platform
- SOC Prime
- SOAR
- DDOS Mitigation
- DFIR
- Use Cases

CYBER INVESTIGATION UNIT
Evidence Leads To More Evidence

A specialized unit dedicated to conducting comprehensive cyber investigation services.

Cyber Investigation Unit will investigate threat events detected in client environments, deliver high quality reports, support client's teams on remote sites, working closely with their own security incident management elements and support the delivery of long-term cyber investigation projects, both on site and remotely. Where necessary, we may also deploy to client sites to undertake cyber related investigations.

UNIT GOALS

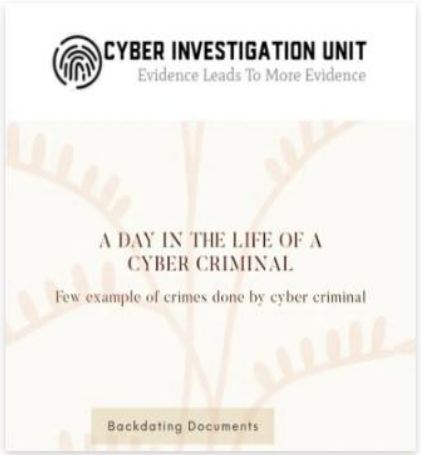
Identify, investigate, and respond to cybercrimes and security incidents, This unit plays a critical role in safeguarding digital assets, ensuring compliance with legal and regulatory standards, and preventing or mitigating harm from cyber threats.

CYBER INVESTIGATION UNIT SERVICES

CYBER ZONES
Cyber Security Services

Proactive Cyber Forensics

A proactive manner aiming to **prevent**, **identify**, and **mitigate cyber threats** before they cause significant damage. The goal of proactive cyber forensics is to reduce the likelihood of cyber incidents, minimize the impact of potential attacks, and help organizations strengthen their overall cybersecurity posture

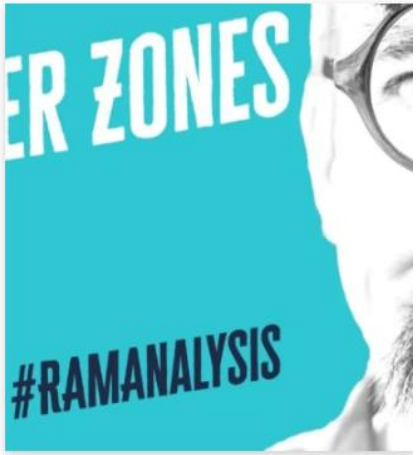


Responsive Cyber Forensics

Traditional forensic investigations, which focus on gathering and analyzing evidence **after** an incident occurs.

Compromise Assessment

Comprehensive evaluation to determine if it has been compromised by malicious actors, The goal of a compromise assessment is to identify any signs of an ongoing or past security breach.

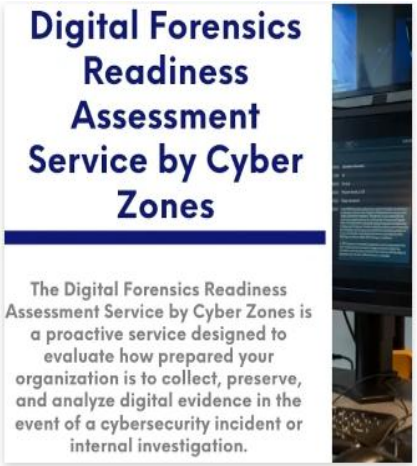


RAM Forensics

Analyzing the contents of a computer's **Random Access Memory (RAM)** to gather evidence or information that can be used in digital investigations, particularly in cases involving cybercrime or security breaches.

CYBER INVESTIGATION UNIT SERVICES

CYBER ZONES
Cyber Security Services

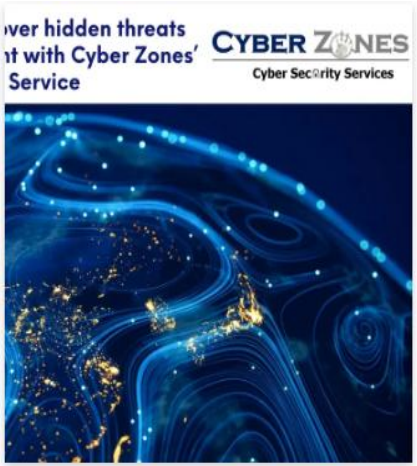


Digital Forensics Readiness Assessment Service

The **Digital Forensics Readiness Assessment Service** by Cyber Zones is a **proactive** service designed to evaluate how prepared your organization is to collect, preserve, and analyze digital evidence in the event of a cybersecurity incident or internal investigation.

Disk Forensics

The **Disk Forensics Service** by Cyber Zones involves the meticulous acquisition, preservation, and analysis of data stored on physical and logical disk drives to uncover digital evidence related to cyber incidents, data breaches, or internal investigations.



Network Forensics Service

The **Network Forensics Service** by Cyber Zones is a specialized digital investigation service focused on capturing, analyzing, and reconstructing network activity to detect signs of compromise, identify threat actors' behavior, and trace unauthorized access or data exfiltration events.

DFIR Program Development Service

The **DFIR Program Development Service** by **Cyber Zones** enables organizations to build and implement a complete, scalable, and mature **Digital Forensics and Incident Response (DFIR)** capability tailored to their environment, risk profile, and regulatory requirements.

Digital Forensics Lab Setup

The **Digital Forensics Lab Setup Service** by Cyber Zones empowers organizations to build an in-house, fully functional, and forensically sound environment dedicated to the collection, preservation, analysis, and reporting of digital evidence related to cybersecurity incidents, legal investigations, and compliance needs.

IOT SECURITY UNIT
CYBER ZONES

Specifically focused on offering advanced cybersecurity services for Internet of Things (IoT) and Operational Technology (OT)

IoT Security Unit specifically focused on offering cybersecurity services for **Internet of Things (IoT)** and **Operational Technology (OT)**

UNIT GOALS

- Strengthen IoT Cybersecurity status
- Develop Comprehensive IoT Frameworks
- Automated Threat Detection
- Regulatory Compliance Assistance
- Covering **IIoT** (Industrial IoT), **IoMT** (Internet of **Medical** Things & Internet of **Military** things) & **CIoT** (consumer IoT)

IoT Cybersecurity Inspection Service

Seeks to pinpoint vulnerabilities in both internal and external assets of clients, enabling our cybersecurity consultants to gain a comprehensive understanding of the protection levels and potential attack surfaces related to our clients' assets in a practical way. This assessment helps to outline a strategic roadmap for both immediate and future actions that clients can take.

IoT Risk Assessment

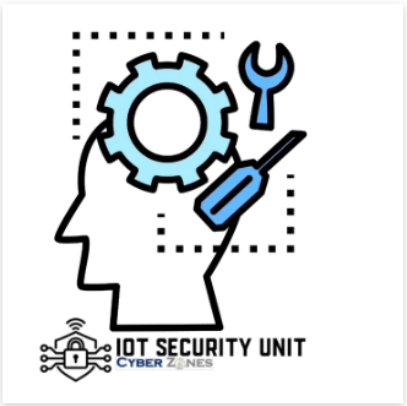
The IoT Risk Assessment service provides a comprehensive evaluation of the security posture of Internet of Things (IoT) devices and networks within your organization.

Endpoint Security

Deploy security measures like encryption, authentication, and monitoring for IoT devices.

Network Segmentation

Aims to provide the recommendation for best way to Isolate IoT/OT networks to reduce the attack surface.



Firmware Management

we will Ensure timely updates and patching of IoT devices based on the classification of the device.

Threat Detection & Response

Use AI/ML-based tools to detect and respond to anomalies.

IoT Compliance Support

IoT Compliance Support service helps organizations navigate the complex landscape of cybersecurity regulations and standards specific to IoT/OT environments. With the increasing adoption of IoT devices, ensuring compliance with local, national, and international regulations—such as **NCA-OTCC**, **GDPR**, **NIST**, and **ISO 27001** has never been more critical.

Develop proprietary frameworks

we specialize in developing customized cybersecurity frameworks for securing IoT and OT environments. These frameworks address the complexities of IoT ecosystems, ensuring robust security across devices and networks. Designed to align with industry requirements and regulations, they incorporate best practices, advanced technologies, and compliance standards for scalable and resilient protection.

TRAINING SERVICE UNIT

CYBER ZONES
Cyber Security Services

Effective cybersecurity training significantly decreases the likelihood of sensitive data being compromised. By educating employees on how to identify and handle potential threats, organizations can protect confidential information from unauthorized access, we have multiple training serves different audience.

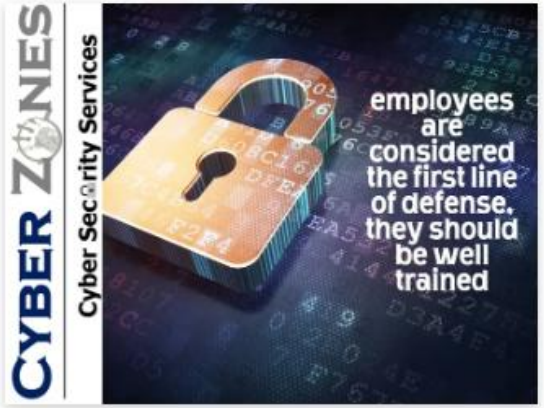
UNIT GOALS

The primary **goal of training service unit** is to equip individuals—whether employees, students, or general users—with the knowledge, practical skills, and awareness needed to protect themselves, their data, and their organization from cyber threats.

CYBERSECURITY AWARENESS

Cybersecurity Awareness for VIP Level

We developed an outstanding training course which aims to provide the prober techniques and latest cyber security threats in a friendly and simple manner to those VIP level.



Cybersecurity Awareness | Non-IT Level

We developed an outstanding training course which aims to provide the prober techniques and latest cyber security threats in a friendly and simple manner to those Non-IT Level.

CYBER SECURITY BASIC & INTRODUCTORY

Cyber Security plus

CS+ training course covers the most important areas that each computer/mobile phone users should know and be aware in order to allow each employee in the company to act as the first line of defense.

Cyber Security First Responder

First Responder prepares the foundation for Cyber security field, it contains in depth details regarding Security and Cyber Security fields, it will prepare the trainee for intermediate courses.

INTERMEDIATE LEVEL | PRACTICAL TRAINING

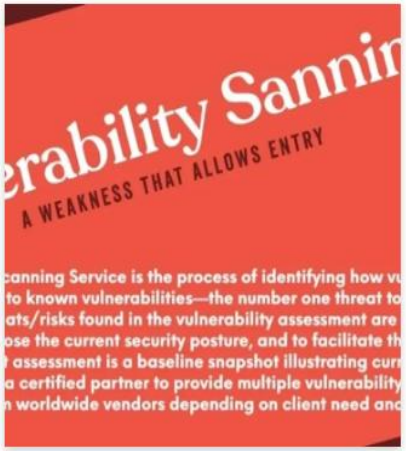
Windows Security Workshop

Windows Security prepares trainees to configure a domain controller and conduct fine tuning to GPO in a pure practical manner, there is no theoretical part as this training is 100% practical.

UTM/Firewall Configuration

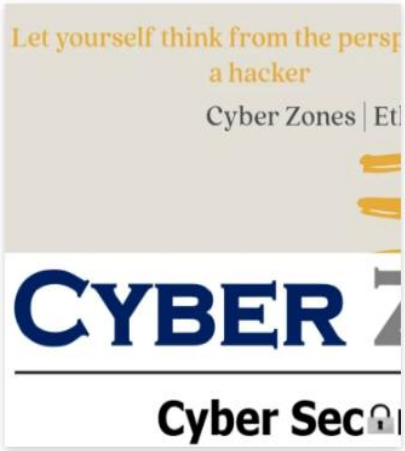
UTM Configuration prepares trainees to configure a UTM and configure firewall policies with protection profiles in a pure practical manner, there is no theoretical part as this training is 100% practical.

RED TEAM TRACK | PRACTICAL TRAINING



Vulnerability Assessment Workshop

Advanced training from **RED training path**, will train student to properly configure and operate OpenVAS.

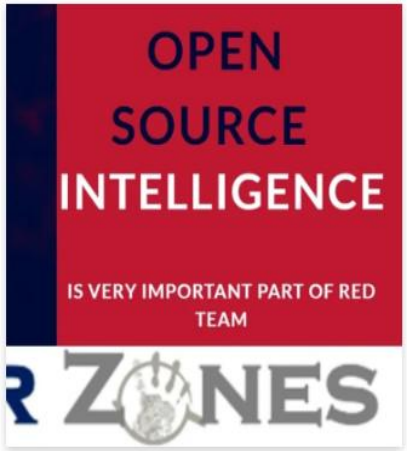


Ethical Hacking Workshop

Advanced training from **RED training path**, will train student to conduct ethical hacking in real case live scenarios.

EHPT Workshop - Consultant Level

Advanced training from **RED training path**, will train student to conduct ethical hacking and penetration Testing engagements in real case live scenarios.



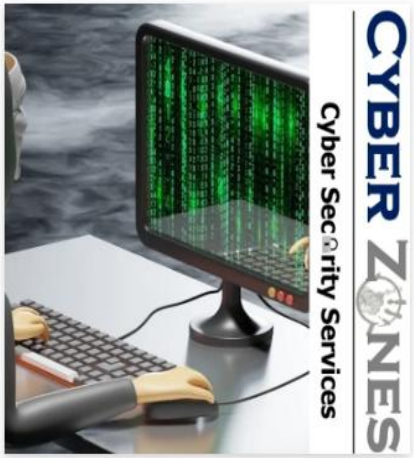
Open-Source Intelligence

Advanced training from **RED training path**, will train student to create his own cat phishing account and start collecting data using open-source technique.

BLUE TEAM TRACK | PRACTICAL TRAINING

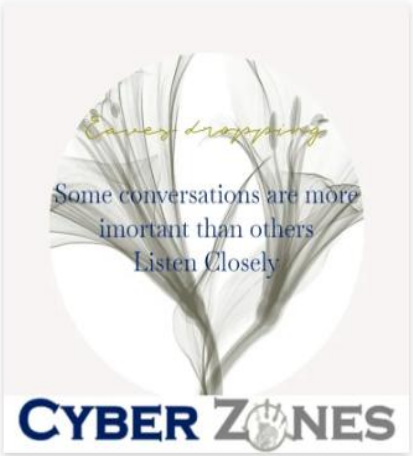
Incident Handling & Response Workshop

Advanced training from **BLUE training path**, will train student to properly respond to real case incidents and conduct live & Network Forensics.



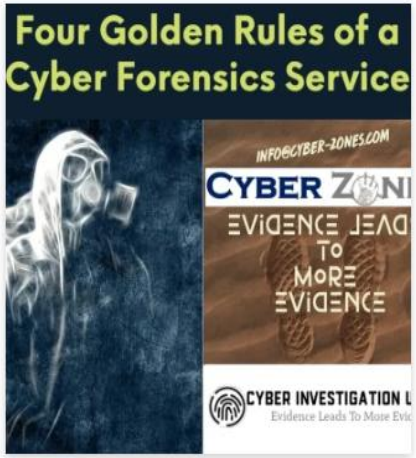
Ransomware Decryption Workshop

Advanced Training from **BLUE Team** training path aims to teach trainees to detect and identify ransomware whereby "trainees" are taught techniques in **a pure practical manner**.



Cyber Threat Intelligence & spyware hunting Workshop

Advanced training from **BLUE training path**, will train student to detect spy software on computers and how to remove the spy software from computers and RAM.



Digital Forensics Workshop

Advanced training from **BLUE training path**, will train student to properly investigate a real case cybercrime in computer systems.

RED TEAM

100% PRACTICAL TRAINING

At Cyber Zones, our world class trainers are battle-tested on the front lines every day. We deliver comprehensive cyber security training that helps the trainees to get real live practical experience, Simply because it is 100% practical training.

RED TEAM

Training Service Unit
CYBER ZONES

From Zero to Hero

CYBER ZONES
Cyber Security Services

RED Team Track

Offensive Security Training Roadmap

BASIC LEVEL

- COURSE 1 | CYBER SECURITY PLUS
- COURSE 2 | CYBER SECURITY FIRST RESPONDER

INTERMEDIATE LEVEL | PRACTICAL TRAINING

- COURSE 3 | WINDOWS SECURITY WORKSHOP
- COURSE 4 | UTM\FIREWALL CONFIRGURATION

ADVANCED LEVEL | PRACTICAL TRAINING

- COURSE 5 | VULNERABILITY ASSESSMENT WORKSHOP
- COURSE 6 | ETHICAL HACKING WORKSHOP
- COURSE 7 | EHPT WORKSHOP - CONSULTANT LEVEL
- COURSE 8 | OPEN SOURCE INTELLIGENCE
- COURSE 9 | BUG BOUNTY WORKSHOP
- COURSE 10 | PENETRATION TESTING WORKSHOP

BLUE TEAM

100% PRACTICAL TRAINING

At Cyber Zones, our world class trainers are battle-tested on the front lines every day. We deliver comprehensive cyber security training that helps the trainees to get real live practical experience, Simply because it is 100% practical training.

www.cyber-zones.com

BLUE TEAM

From Zero to Hero

CYBER ZONES
Cyber Security Services

Blue Team Track

Defensive Security Training Roadmap

BASIC LEVEL

- COURSE 1 | CYBER SECURITY PLUS
- COURSE 2 | CYBER SECURITY FIRST RESPONDER

INTERMEDIATE LEVEL | PRACTICAL TRAINING

- COURSE 3 | WINDOWS SECURITY WORKSHOP
- COURSE 4 | UTM\FIREWALL CONFIRGURATION

ADVANCED LEVEL | PRACTICAL TRAINING

- COURSE 5 | INCIDENT HANDLING & RESPONSE WORKSHOP
- COURSE 6 | RANSOMWARE DECRYPTION WORKSHOP
- COURSE 7 | CYBER THREAT INTELLIGENCE & SPYWARE HUNTING
- COURSE 8 | DIGITAL FORENSICS WORKSHOP
- COURSE 9 | MOBILE FORENSICS WORKSHOP
- COURSE 10 | CYBER FORENSICS EXAMINER WORKSHOP

Training Service Unit
CYBER ZONES

ONLINE APPOINTMENTS

Blue, RED, Gold, Purple, White and Black Team drills

Online meeting Related to Cyber Advisory Unit Services

1 hr | Free

Experience seamless online meetings with our Advisory Unit services. Stay connected, collab and protect your business from cyber

Cybersecurity awareness training, BLUE and R team track specialization

Online meeting Related to Training Services Unit

1 hr | Free

Experience seamless and secure online meetings Training Services Unit. Stay ahead in CyberSec with our professional virtual ses


THANK
YOU