CYBEROZONE

Securing Generations

Cyber Security
Consulting and Services

www.cyberozone.com

ABOUT US

We at Cyberozone are a one-stop solution to get all your security needs. As your business ecosystem and value chain expand, we help you address essential elements of cybersecurity, from strategy, enterprise risk management, implementation, and management.

Our team is enriched with experts who share our passion and values and have a thirst for empowering business with their wealth of knowledge and experience in the latest developments in Cybersecurity solutions.

Our mission is to move cybersecurity in the right direction by defending and providing enterprise-grade solutions to customers to reduce their threat landscape to digital age business.

BUSINESS VALUE

Security Compliances

Data Protection

Business Continuity

Reputation Protection

Risk Management

OUR STRENGTHS

- Expertise in handling latest cyber security challenges.
- Team of Experienced & Certified Professionals
- Expertise to secure multiple industries.
- Backed with complete cyber security process.

OUR APPROACH

Consulting:

- Understanding Existing Infrastructure
- Discuss future company's IT requirements
- Understand the security specific requirements
- Identify the Gaps
- Balance Costs and measures

Planning:

- Creating Plan of Action
- Understand the working hours and Identify down time for update
- Impact analysis
- Backup and Recovery Planning
- Testing mode and live changes

Implementation

- Creating Guideline for Implementation
- Follow the plan of action
- Full scope Implementation
- Security Project Management
- Project Review

Consultation | Analysis | Planning | Solutions | Implementation

Analysis:

- Analyze the existing solutions
- Identifies the dependencies
- Mapping to the security requirements
- Classify the requirements and gaps

Solutions:

Strategic:

- Checking the best suitable solution
- Reduce the security risk
- Improve all over IT Infrastructure
- Reduce IT Cost
- Optimize business process
- Meet the IT Standards and compliances

Technical:

- Infrastructure and Network Security
- Cloud Security
- Application Security
- Identity and Access management
- Business continuity management
- Compliance audit and management
- Data Security

Support:

- Knowledge transfer
- Guideline for manage
- Standard Operating Procedures (SOP)
- Annual Maintenance Contract (AMC)

Right approach towards cyber security will always make you safer.

We deliver cyber security solutions to customers in a way to provide highest level of security through the full process from consulting, solutions to support.

CONSULTING

- **1 in 4 – that is how high one's odds are of becoming a victim of a cyberattack. With a new cyberattack happening every 39 seconds now.**
- **Cybercrime will cost the world $6 trillion by 2021.**

Cybersecurity

Infrastructure and network security

Data Security

Cyber Forensics Investigation

Cyber Crime & Legal

Web and mobile app security

Cloud Security

Data Recovery and Backup

Incident Management

Security Operation Center(SOC)

Managed Security services (MSS)

IoT Security

Risk Assessment and Management

Security Audits

INFORMATION & NETWORK SECURITY

- **There will be 45 trillion networked sensors in 20 years.**
- **By 2021, a business will fall victim to ransomware every 11 seconds.**
- **The cost of lost business averaged $1.52 million. (IBM)**

Secure Network Architecture Design

Design the secure network architecture according to the security standards and industry specialize solutions. This secure architecture will help to prevent cyber attack in organization.

Firewall(IDS/IPS)

Firewall is the first line of defence in you internal network to the internet and outer world. Strong and well configure firewall make it difficult for hacker to enter to your network.

Network Security Audit

Network audit will help to identify the flows and the vulnerability in the network. Which can be patch and resolved according to it's severity.

Infrastructure Security Audit

Infrastructure audit will help to identify the flows and the vulnerability in full IT Infrastructure. Which can be patch and resolved according to it's severity.

Benefits

- Reducing operating and capital expenditures.
- Reducing infrastructure and Network costs
- Protecting business from disruption.
- Protecting Reputation

Softwares

Firewall :

FORTINET, GAJSHIELD, Check Point, SOPHOS, paloalto

Backup and Disaster recovery :

Acronis, vembu BDR

Remote Desktop :

Netop

Network Security :

Nessus vulnerability scanner, OpenVAS

WEB & MOBILE APP SECURITY

- **The number of mobile ransomware infections increased by 33% in 2018.**
- **Symantec blocked an average of 10,573 malicious apps every day in 2018.**
- **63% of all mobile ransomware infections are in the US.**

Web App Security testing / audit

Thousands of websites and webapps are getting hacked daily due to lack of security.

Webapp security testing will help to identify vulnerability, any loophole in code, vulnerability in the platform upon which website or web app is developed. Once found it can be resolved with best practices.

For that Web App Vulnerability assessment (VA) or Web App Vulnerability assessment Penetration Testing (VAPT) will be effective.

Which include manual and automated security tests to secure websites and web app on any underlying platform. This practise also include to identify security issues on web server where web app or website hosted on.

Mobile app Security

Mobile apps are a new market for all your needs. From shopping to banking, mobile apps are used widely for app purposes. As the use of mobile apps are increasing the security threats are also increasing. The mobile app pentesting will prevent you from the losses.

- Android app Vulnerability assessment (VA)
- Android app Penetration testing (VAPT)
- iOS app Vulnerability assessment (VA)
- iOS app Penetration testing (VAPT)

Benefits

- Ensuring application quality to support reputation and competitive advantage
- Reducing costs of application security – decrease security incidents
- Ensuring business continuity and application sustainability
- Securely provision mobile devices to users
- Provide secure tunneling to the enterprise.

Softwares

Web application firewall :

Prophaze, Barracuda, imperva, CLOUDFLARE

Web app security :

acunetix, RAPID7, KALI LINUX, metasploit, nessus Professional, Burp Suite, OWASP

RISK COMPLIANCE

- **88% of companies spent more than $1 million on preparing for the GDPR. (IT Governance)**
- **The cost of a data breach will reach $150 million by 2020.**
- **Since the GDPR was enacted, 31% of consumers feel their overall experience with companies has improved. (Marketing Week)**

GDPR Guideline

The GDPR (General Data Protection Regulation) was adopted by the European Parliament as of April, 2016. The types of private data which the GDPR would protect include primary identity information (like, name, address, ID numbers), web data (like, location, cookie data, IP address, RFID tags), health and genetic data, racial or ethnic data, sexual orientation, biometric data and political opinions.

PCI DSS

All organizations that process, retain or transmit customer information including credit card data have an obligation to meet PCI-DSS (Payment Card Industry Data Security Standards) requirements.

ISO 27001

ISO/IEC 27001 is an international standard on how to manage information security. International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organizations make the information assets they hold more secure.

HIPAA

Health Insurance Portability and Accountability Act It was created primarily to modernize the flow of healthcare information, stipulate how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft.

Data Privacy assessment and audit

Data privacy includes how data is collected, processed, stored, maintained, protected and disposed of irrespective of the format and systems used.

Softwares

Data Leak :

Data Resolve · Symantec · falcongaze · McAfee · SOMANSA

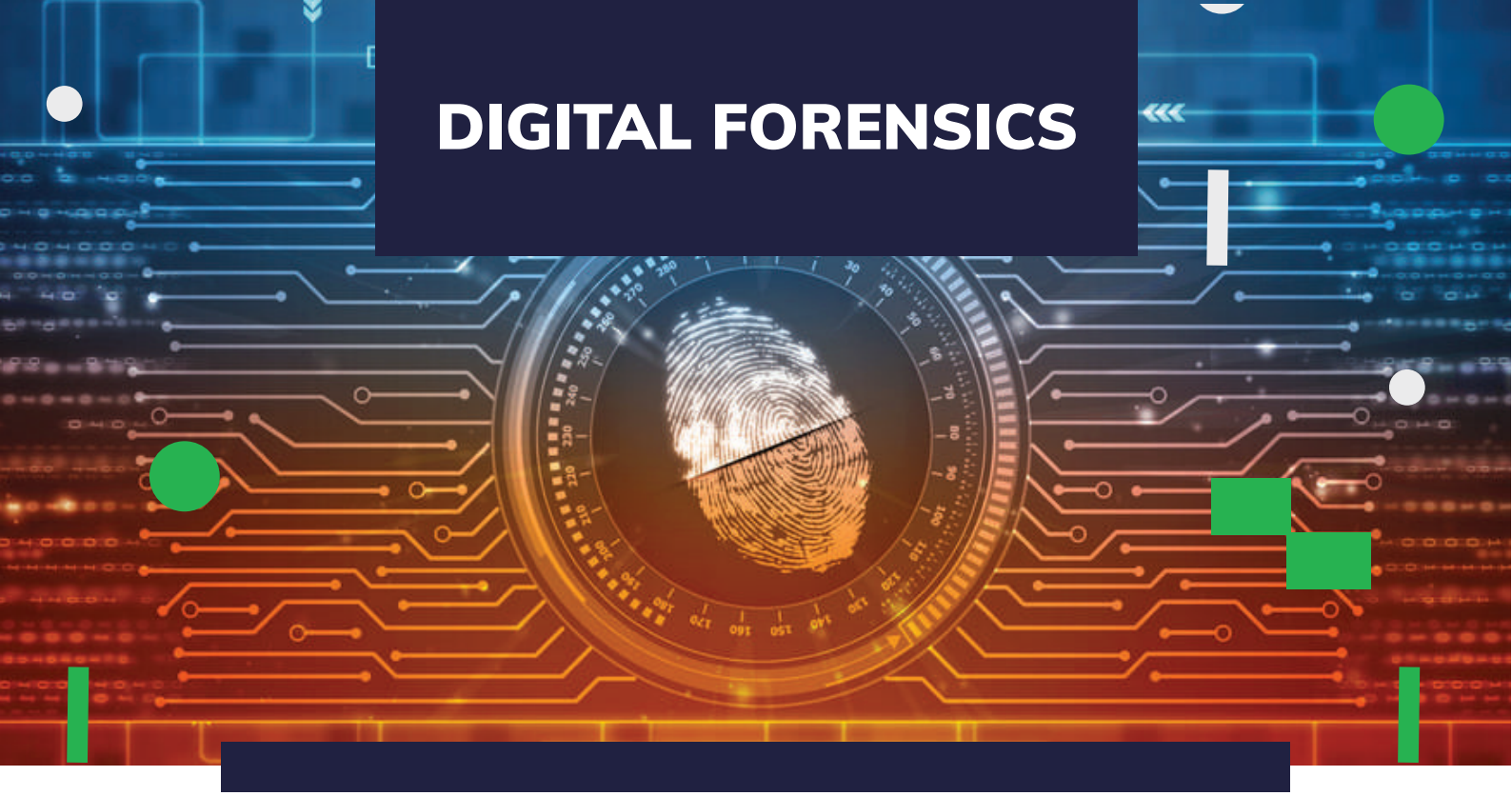
Compilance :

PCI DSS · ISO · GDPR · COBIT 5 · HIPAA · NIST

Authentication :

WatchGuard · DUO · LastPass · SECUREAUTH · RSA · Google Authenticator

DIGITAL FORENSICS



E-mail Forensics

E-mail forensic analysis is used to study the source and content of an e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, and more.

Windows Forensics

Windows forensics knowledge of Microsoft Windows operating systems by analyzing and authenticating forensic data as well as track detailed user activity and organize findings.

Log Forensics

Log forensics means using log analytics in forensics. In other words, it means to perform analysis on log entries, in order to extract knowledge and insights from them, but with a very specific goal in mind: to establish factual information for judicial review.

Mobile Forensics

Mobile forensics is a branch of digital forensics related to the recovery of digital evidence from mobile devices. “Forensically sound” is a term used extensively in the digital forensics world to qualify and justify the use of a particular forensic technology or methodology. Covering both Android and iOS devices.

Also working on other types of forensics like Memory Forensics, External storage Device forensics, Memory Forensics, Live digital Forensics and Data Theft & Document forgery Investigation.

Softwares

Digital Forensics :

prodiscover® COMPUTER FORENSICS

SANS DFIR

X-Ways

WIRESHARK

ARSENAL RECON

VOLATILITY

Xplico

e-fense CARPE DATUM

CROWDSTRIKE

SECURITY MONITORING & SIEM

- **Enterprises lose $4.7 million to cybercriminals annually.**
- **Enterprise spending on cloud security solutions is predicted to increase from $636M in 2020 to $1.63B in 2023, attaining a 26.5% CAGR. (Gartner)**
- **Security Information and Event Management (SIEM) market size is expected to grow from USD 4.2 billion in 2020 to USD 5.5 billion by 2025**

Asset Discovery

- Active and Passive Network Scanning
- Asset Inventory
- Assent visibility

Vulnerability Assessment

- Continuous Vulnerability Monitoring
- Authenticated / Unauthenticated Active Scanning

Threat Detection

- Network and Wireless IDS
- Host IDS
- File Integrity Monitoring
- Advanced Persistent Threat Detection

Behavioral Monitoring

- Log Collection
- Netflow Analysis
- Server and Service Availability Monitoring

Security Intelligence / SIEM

- Log analysis
- Log management
- SIEM Event Correlation
- Incident Response

Benefits

- Improved Risk Management (monitoring, detection and response)
- Cost effective (usage of popular open source security tools)
- Access to a team of certified specialists
- Flexible and scalable to suit any size business
- “Pay as you grow” license model
- Open source model for cost reduction

Softwares

Security Monitoring and SIEM :

splunk> · AlienVault · exabeam · LogRhythm · IBM QRadar · ArcSight · SECURONIX

Open Source :

elastic stack · WAZUH · SOS

Log management :

sumo logic · solarwinds LOGGLY · elastic stack

SERVER SECURITY

- **DDoS attacks on servers can cost enterprise organizations $50,000 in lost revenue from downtime and mitigation costs.**
- **An unsecured server exposed the sensitive data belonging to 60,000 customers of the family history search software company, Ancestry.com (IdentityForce).**
- **Facebook had 540 million user records exposed on the Amazon cloud server (CBS).**

Hardware

We will help you to get suitable server hardware for long term use and sustainability. Proper server hardware help to get better ROI

Configurations

Configure server expertise and we have a team of specialists in the industry who will help you to configure servers according to business requirements. We also have an expert team for VMWare configurations.

Backup

Server backup will help to prevent loss and help to recover in critical time. Inhouse or cloud backup solutions can be designed for high availability of Infrastructure.

Disaster Recovery

Recovery solution that will help you in the worst case scenario. This recovery will help to get back to last saved

Security

Server security should be the highest priority for any organization. Which contain an endpoint security solution and firewall in the network. DMZ zone is suggested for highest level security for servers.

Benefits

- Reduced the of server related attacks
- High availability of server
- Secure Infrastructure and application
- ROI from Infrastructure

Softwares

Hardware :

Hewlett Packard Enterprise, DELL, Lenovo, IBM

Configuration :

Windows Server, redhat, vmware

Cloud Backup :

IDrive, BACKBLAZE, Acronis True Image

CLOUD SECURITY

- **70% of organizations hosting data/workloads in the public cloud experienced a security incident.**
- **66% of organizations leave back doors open to attackers through misconfigured cloud services.**
- **90% of companies are on the cloud**

Cloud Configuration

Configuration in Cloud platforms like Amazon AWS, Google cloud platform and Microsoft Azure. Solution for cloud IaaS, PaaS and SaaS.

Storage

Secure cloud storage becomes important as companies are migrating their storage to cloud. We help to securely migrate your storage and make it secure on the cloud by cutting edge solutions.

CDN

CDN will help faster load times for web and mobile users and also quickly scalable for heavy traffic. Secure CDN solution will help to increase the speed and security together.

Security Configuration

Cloud is as vulnerable as your traditional server and system. By using a proper set of products, tools and security configuration we can make it a secure place for all businesses.

Cloud Security Audit:

As like on-premise infrastructure, the cloud requires a security audit to make sure it's secure enough. Cloud security audit will help to figure out vulnerability and miss-configuration which can lead to big losses.

Benefits

- High Availability
- Secure access of Application or data from anywhere from any device
- Speed, Security, availability
- Secure from all latest threats

Softwares

Cloud :

aws · Google Cloud · Azure

Backup :

IDrive · BACKBLAZE · Acronis True Image

Storage :

amazon S3 · Google Drive · OneDrive

CDN :

amazon cloudfront · CLOUDFLARE · TATA

WAF :

Prophaze · Barracuda · imperva

ENDPOINT SECURITY

- **68% of organizations were victims of endpoint attacks in 2019**
- **42% of all endpoints are unprotected at any given time**
- **The endpoint security market is expected to grow at a CAGR of 5.9% from 2020 to reach $18.6 billion by 2027**

Anti virus

Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

Anti Malware

Antimalware is a type of software program created to protect information technology (IT) systems and individual computers from malicious software, or malware. Antimalware programs scan a computer system to prevent, detect and remove malware. A wide variety of malware types exist, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, rogue software, wiper and scareware.

Endpoint detection and response (EDR)

Endpoint detection and response (EDR) is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. Key Features include Filtering, Advanced Threat Blocking, Incident Response Capabilities, Multiple Threat Protection.

Benefits

- Securing end-point device from Ransomware
- Securing from Zero-day threats Business continuity
- Securing employee and company data
- ROI

Softwares

Antivirus :

Bitdefender kaspersky Norton eset avast McAfee TREND MICRO

Anti-malware :

EMSISOFT kaspersky Malwarebytes TREND MICRO

EDR :

CROWDSTRIKE SentinelOne McAfee Carbon Black. FIREEYE TREND MICRO

EMAIL SECURITY

- **94% of malware is delivered via email. (CSO Online)**
- **The average ransomware payment rose 33% in 2020 over 2019, to $111,605. (Fintech News)**
- **48% of malicious email attachments are office files. (Symantec)**

Email Server Setup

We will help out to configure email servers on premise or on cloud with all necessary enterprise requirements.

Email Backup

Email backup processes and stores emails in a safe, centralised location. Emails can be stored securely and retrieved, unchanged, at any time. Email backup helps prevent data loss by enabling users to restore email content that potentially has been deleted or lost. Backups keep your email messages available for longer, and make tracking down lost emails much quicker.

Email Security gateway

An email gateway is a type of email server that protects an organization or users internal email servers. This server acts as a gateway through which every incoming and outgoing email passes through. A Secure Email Gateway (SEG) is a device or software used for email monitoring that is being sent and received. Email Gateways will help to protect from social engineering attacks such as phishing, or business email compromise also from ransomware and malicious attachments.

Benefits

- Seamless and secure Email communication
- Data Security
- Privacy of company

Softwares

Email Server :

Gmail, PostMaster Enterprise, axigen, Office 365

Email Backup :

Dropsuite, MailStore

Email Security Gateway :

Cisco, Barracuda, mimecast, proofpoint, AVANAN

DARK WEB MONITORING

- **Over 94% of the world's information resides in the deep and dark webs.**
- **Over 21 million of corporate accounts belonging to Fortune 500 companies were breached and put for sale in Dark Web in 2019**
- **60% of the information available on the Dark Web could potentially harm enterprises.**

Email Credentials

Email security is one of the important parts of any business. We will help to identify email addresses against a database of breached credentials to see if they have been involved in any breaches. So credentials can be change as soon as possible and prevent from big loss.

Confidential Data

Confidential data is companies utmost sensitive information that you don't want anyone to obtain without your permission. This may include Employee information, client data, companies financial information, website details, Project information and more.

Misuse of Brand Identity

Misuse of Brand name, Logo, tagline, license Products or more. In the dark web it can be use and it will affect the integrity of Brand name.

Copyright

A copyright is a collection of rights that automatically vest to someone who creates an original work of authorship like a literary work, song, movie, drug, book or software. These rights include the right to reproduce the work, to prepare derivative works, to distribute copies, and to perform and display the work publicly.

Financial/Banking Information

Dark web contains hacked data of financial and banking information like account details, address, email, mobile number, banking credentials, credit card/ debit card number, CVV number and more.

Medical Information

Some of the hacks of medical institutes or technological companies contain the medical information of patients and it can be then leveraged in many ways.

Benefits

- Secure intellectual properties
- Data leak prevention
- Secure brand reputation
- Client Data protections

MANAGED SECURITY SERVICES

- **According to a research by the Cybercrime Magazine, the cost of cybercrime will reach 6 trillion dollars worldwide by 2021, and the cost of ransomware damages will rise to 20 billion dollars.**
- **95 percent of security breaches happen because of human errors.**
- **In 2020, 17 percent of breaches involved malware, 22 percent featured phishing attacks, and 45 percent were hacking.**

Consulting

Customized assistance in the assessment of business risks, key business requirements for security and the development of security policies and processes. It includes technology, business risks, technical risks and procedures.

Security Management

Managing all the security devices like firewall, IPS, IDS next generation firewall and other security devices. We protects devices and data and provides continuous security monitoring and operational administration of managed devices to safeguard investments and meet compliance regulations.

Advanced Threat Management

It includes Advanced Endpoint Threat Detection (AETD), Advanced Endpoint Threat Prevention, Advanced Remediation Management. It will help to Prevent cyber threats that leverage the vulnerability of end-point and known or zero-day.

Compliance Monitoring

Compliance monitoring is an important part when it needs to monitor continuity of compliance like PCI, GDPR, HIPAA, ISO/IEC 27001.

Security Monitoring

This is the day-to-day monitoring and interpretation of important system events throughout the network—including unauthorized behavior, malicious hacks, denial of service (DoS), anomalies, and trend analysis. It includes Log Management & Compliance Reporting and security event monitoring.

Pentesting & Vulnerability Management

This includes one-time or periodic software scans or hacking attempts in order to find vulnerabilities in a technical and logical perimeter. It includes services like Vulnerability Program Management, Vulnerability Scanning, Web Application Scanning and Network pen-testing.

Benefits

- Next-generation security technologies
- ROI
- Business Continuity
- Protection from Advance threat
- Proactive managed security

SPECIAL SERVICES

Cyber crime costs organizations $2.9 million every minute, and major businesses lose $25 per minute as a result of data breaches, according to RiskIQ research.

98% of IoT Traffic Isn't Encrypted

45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)

Annual Security+ Maintenance service

This includes regular security checks of Infrastructure and network of company, identify the gaps and provide solutions, provides updates and patches where required, find and apply optimal solutions for smooth operations.

IoT security

IoT security is the act of securing Internet of Things devices and the networks they're connected to. In the business setting, IoT devices include industrial machines, smart energy grids, building automation, plus whatever personal IoT devices employees bring to work.

Ransomware Threat Response

Ransomware is a type of malicious software (malware) that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. It can be proactively secure by End-point security solutions.

Virtual CISO

A virtual CISO (vCISO) can bring both strategic and operational leadership on security to companies that can't afford a full-time person in the role. Gain day-to-day cyber security support and counsel from a dedicated vCISO along with long-term security strategy, vision, program and policy design, and implementation.

Cyber Crime Investigation

a cybercrime investigation is the process of investigating, analyzing and recovering critical forensic digital data from the networks involved in the attack

Data backup and Recovery

Data backup and recovery is the process of backing up your data in the event of a loss and setting up secure systems that allow you to recover your data as a result.

Social Media Investigation

A social media investigation looks into the social media posts, status updates, photos, and conversations of an individual. You might require a social media investigation for a court case, custody battle, or as part of a background investigation.

INDUSTRIES

- More than 93% of healthcare organizations experienced a data breach in the past three years. (Herjavec Group)
- 87% of Higher Education And Schools have experienced at least one successful cyber attack
- The financial services industry takes in the highest cost from cybercrime at an average of $18.3 million per company surveyed. (Accenture)

Banking

Finanace

Health Care

Education

Manufacturing

E-Commerce

Government

Oil and Energy

Technology

Pharma

Retail

Gaming

Block Chain

Real Estate

Hostel

Travel