C-YBER®

Cybersecurity services

www.c-yber.com

We face constant threats, tough IT rules, and we rely more and more on services in the cloud.

At C-YBER we pinpoint possible threats and protect against cyber-attacks. With us, your online environment is resilient.

Threat Landscape and Cybersecurity Challenges in the Industry

Cyber threats aren't just hypothetical - they're an actual menace confronting every sector today. These harmful assaults have resulted in losses amounting to hundreds of millions of dollars for businesses around the world. Moreover, perpetrators of these threats continually innovate new strategies to infiltrate information and operational systems.

Companies are increasingly likely to face these cyber-attacks. Hence, to shield their assets, operations, and people from such impending hazards, it's vital for firms to devise an effective cybersecurity strategy. It's equally important to seamlessly embed cybersecurity safeguards into their daily processes.

Cyber-attacks companies are most likely to face

Unpatched software	A digital doorway left open, inviting in a myriad of cyber threats.
Socially engineered threats	The psychological ploys designed to exploit human trust, highlighting the importance of comprehensive security awareness training.
USB and other removable media	Potentially dangerous vessels of data, masquerading as harmless tools, underscoring the need for stringent device control.
Advanced Persistent Threats (APT)	Your silent adversaries, nestled within your network, strategizing and striking with precision, underlining the necessity for relentless vigilance.
Phishing attacks	Digital snares artfully crafted to deceive and ensnare, emphasizing the crucial need for advanced email security solutions.

Challenges

Maintaining a robust security framework involves multiple hurdles. Incident response requires rapid, effective solutions to cyber threats, often complicated by evolving attack techniques. Application security presents challenges in balancing usability with security, requiring constant patching and vulnerability management. **To become more resiliant to cyber security attacks it is important to have mulity layerd approch to protection.**

Cyber Security Resiliance Layers

Cybersecurity services that we offer

Given that every IT infrastructure is unique and sophisticated cyberthreats are specifically crafted to target the distinctive weaknesses of each organization, our professional services are customized accordingly. The solutions outlined in the subsequent pages constitute a portion of our extensive portfolio - these services, either in their entirety or in parts, may be leveraged during our collaboration with you.

Key solutions

Penetration Testing

Advise | Implement

We simulate cyber attacks to identify and remedy system vulnerabilities

API Penetration Testing

Advise | Implement

Evaluating and securing API endpoints against potential threats for optimal data protection.

Application Security Engineering

Advise | Implement

Protecting applications via threat modeling, secure practices, testing, deployment, and OWASP ASVS

Cloud Security

Advise | Implement | Manage

Protect cloud data, network, identities, ensure compliance, respond to incidents, utilize top providers.

Incident response

Advise

Incident response in cybersecurity involves preparation, detection and analysis of threats, containment and eradication of breaches, recovery of systems, and post-incident,evaluation for improved future security measures.

Digital forensics

Advise | Implement

Digital forensics investigates digital data, collecting,examining, and analyzing it, for legal cases and cybersecurity incidents, while maintaining evidence integrity.

Penetration Testing

Penetration testing, or "pentesting," is a simulated cyber attack against your computer system, network, or web application. It's designed to test defenses and spot vulnerabilities that a hacker could exploit. Rest assured, this process is executed with the owner's full consent and always complies with the law.

A typical penetration test involves six key steps:

1 Planning

The testing scope is defined, covering the systems, networks, and applications to be tested, along with any specific rules

2 Reconnaissance

The pentester gathers data about the target system, its network architecture, and potential weaknesses.

3 Vulnerability Assessment

Tools are used to identify vulnerabilities like software issues, misconfigurations, and insecure practices.

4 Exploitation

These identified vulnerabilities are exploited to gain access.

5 Post-exploitation

If access is gained, the tester escalates their privileges and accesses more resources.

6 Reporting

A detailed report is prepared, summarizing findings, exploited vulnerabilities, and recommendations for remediation.

Where Can We Apply It?

Penetration tests can be executed in a production environment (a live system) to identify real-world vulnerabilities or a development environment (during the development phase) to spot vulnerabilities in code and applications.

What Do You Get?

The outcome includes an executive summary, a detailed report, a list of vulnerabilities, exploit documentation, a remediation plan, and a presentation to the client.
Duration The duration of a penetration test varies but careful planning ensures it meets the client's expectations.

Testing Approaches Several approaches exist for a penetration test

- **Black, Gray, and White Box Testing:** Depending on the tester's knowledge level about the system.
- **External and Internal Testing:** Simulating an attack from outside or within the organization.
- **Targeted Testing:** Focusing on a specific system, network, or application.

API Security testing

Deliverables from API Security Testing

Key outcomes include a test plan, detailed test cases, test report, vulnerability assessment report, proof-of-concept exploits, remediation recommendations, and other artifacts to support findings.

How Long Does It Take?

Duration depends on API complexity, scope of testing, testing approach, resource availability, collaboration efficiency, test environment setup, and time for reporting and remediation. It can range from a few days to several weeks.

What is API Security Testing?

APIs are integral parts of modern software that enable applications to communicate and share data. API security testing is the process of identifying and addressing vulnerabilities that could compromise data safety. It aims to prevent unauthorized access, data breaches, and other security threats.

What Does API Security Testing Cover?

Key areas include:

- **Authentication and Authorization:** Ensures only authorized access to API endpoints.
- **Input Validation:** Prevents common vulnerabilities like injection or XSS attacks.
- **Encryption and Data Integrity:** Validates secure transmission and integrity of data.
- **Rate Limiting and Throttling:** Stops potential abuse or DoS attacks.
- **Error Handling and Logging:** Checks secure error management and effective logging for incident detection.
- **Third-Party Integrations:** Evaluates risks associated with external service integration.
- **Security Headers:** Examines security headers like CSP, CORS, and HSTS in API responses.

The API Security Testing Process

Involves steps like requirement analysis, threat modeling, test environment setup, testing of various aspects (like authentication, encryption, error handling, etc.), vulnerability scanning, and reporting.
Role of OpenAPI Schema This acts as a blueprint for API, aiding in test coverage, test orchestration, input/output validation, verification of security controls, and effective documentation and collaboration.

Application Security Engineering

Application Security Engineering is your best line of defense against potential threats and vulnerabilities. It ensures your applications are designed, built, and maintained securely, and that protective measures are integrated throughout the Software Development Life Cycle (SDLC). Prioritize security, and protect your systems and data from potential attacks!

Stay ahead of threats with our comprehensive approach:

1 Threat Modeling

Identify potential threats, their likelihood, and impact.

2 Secure Coding Practices

Use secure programming languages and control measures like input validation, authorization controls, and secure handling of sensitive data.

3 Security Testing

Perform penetration testing and code review to uncover vulnerabilities.

4 Secure Deployment

Use secure protocols and set appropriate access controls.

5 Maintenance & Updates

Perform regular maintenance, patch vulnerabilities, and monitor for threats.

Meet OWASP ASVS: Your Guide to Application Security

The Open Web Application Security Project's Application Security Verification Standard (ASVS) is a detailed set of security controls and requirements to ensure the security of your web applications. With ASVS, you can establish security baselines, assess application security, and verify security before deployment.

ASVS Risk Levels: Tailored for Your Needs

ASVS provides four risk levels, each tailored to suit the data sensitivity and potential impact of a security breach. Ranging from Level 1 (lowest risk) for applications handling low-sensitivity data, up to Level 4 (highest risk) for applications dealing with extremely sensitive data and with a high organizational impact. Choose what's right for you!

ASVS Audits: Validate Your Security

ASVS audits are thorough evaluations of your application's security against the requirements of ASVS. They reveal vulnerabilities and ensure you meet necessary security standards. An ASVS audit, coupled with ongoing maintenance and updates, is the key to long-lasting application security.

Cloud Security

Cloud security is your safeguard against digital threats. It encapsulates the methods used to protect your data, applications, and infrastructure within the cloud, preventing unauthorized access, alteration, or destruction.

Top Cloud Security Providers

Cloud platforms like Google Cloud, Microsoft Azure, and Amazon Web Services (AWS) offer a range of security products and services, including network security services, identity and access management services, key management services, and security management platforms.

Why is Cloud Security Vital?

With the cloud frequently storing sensitive data such as personal, financial, or medical information, data protection is paramount. Furthermore, businesses must comply with data security laws, regulations, and industry standards. A security breach could seriously harm a company's reputation and trust with stakeholders. Additionally, a security incident can disrupt business continuity. That's why cloud security is no longer optional but essential.

Key Components of Cloud Security:

- **Data Security:** Techniques such as encryption and access controls keep data safe.
- **Network Security:** Measures like firewalls secure the infrastructure connecting cloud resources.
- **Identity and Access Management:** Control access to cloud resources based on user identity and permissions.
- **Compliance:** Ensure cloud operations adhere to relevant laws, regulations, and industry standards.
- **Incident Response:** Have a plan to manage and reduce the impact of security incidents.

Implementing Cloud Security

The implementation process can vary, but it typically includes assessing current security posture, developing a security strategy, implementing security measures, and regular testing and monitoring. It's generally recommended to work with a cloud security expert or a managed service provider to ensure effective and efficient implementation.

Incident Response

Incident response in cybersecurity is an essential process for managing security breaches or cyber attacks. Its goal is to minimize damage, lower recovery time and costs, and reduce any adverse impact on your organization's operations or reputation.

The Process of Incident Response:

1 Preparation

Establish an incident response team, design response plans, and implement preventative measures. It's all about being ready before an incident occurs.

2 Detection and Analysis

Monitor system logs, identify unusual activity, and analyze behavior patterns. The aim is to spot a breach promptly and accurately.

3 C.E.R

C.E.R stands for Containment, Eradication, and Recovery. Limit the incident's impact, remove the threat, and restore systems to a secure state. The focus is on swift and effective action to prevent further damage.

4 Post-Incident Activity

Review the incident, assess the response's effectiveness, and glean lessons for future incident response efforts. It's all about learning and improving.

What to Expect from Incident Response

The outcomes of an incident response process are integral to improving your organization's security measures. These include:

- **Incident Response Plan**: A blueprint for identifying, responding to, and recovering from security incidents.
- **Incident Identification and Reports:** Evidence and detailed accounts of the security incident.
- **Incident Review and Analysis:** A thorough evaluation of the incident and effectiveness of the response.
- **Recovery and Restoration Plans**: Steps to safely restore affected systems and prevent future incidents.
- **Communications:** Keeping stakeholders informed is key.
- **Lessons Learned and Updates:** Based on lessons learned, recommended changes to improve security.
- **Forensic Evidence and Legal Documentation:** In case of legal investigations, the preservation of evidence is crucial.

Factors Influencing the Duration of Incident Response

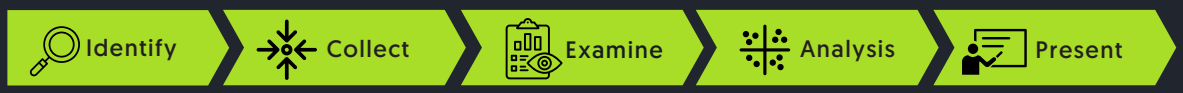
Several factors influence the time taken for incident response, including the severity and scope of the incident, detection time, available resources and expertise, and stakeholder cooperation. On average, a breach identification and containment take around 287 days, but individual cases can vary.

Incident response is not just about managing the immediate aftermath, but also about improving the organization's overall security posture for the future.

Digital Forensics

Digital forensics, a specialized branch of forensic science, is all about investigating digital data to assist in legal cases and cybersecurity incidents.

The Digital Forensics Process:



1 Identification

Find the digital devices holding potential evidence.

2 Collection

Acquire and protect the data securely.

3 Examination

Scrutinize the data using forensic techniques..

4 Analysis

Interpret the findings to reconstruct events and user activities.

5 Presentation

Report the findings clearly and sometimes provide expert testimony in court..

What Do Digital Forensic Analysts Do?

Digital forensic analysts are tech-savvy professionals who extract data from various sources like computers, mobile devices, and networks. They use a methodical approach to ensure data integrity and comply with legal standards.

Key Deliverables:

- **Forensic Report:** Detailed report of the entire investigation.
- **Evidence Preservation:** Properly stored and validated digital evidence.
- **Chain of Custody Documentation:** Records detailing the handling of digital evidence.
- **Recovered Data and Artifacts:** Data and artifacts recovered from various digital sources.
- **Timeline and Reconstruction Analysis:** Timelines or reconstructed sequences of events related to a crime.
- **Expert Testimony:** Expert accounts in court explaining the investigation findings.

Project Duration:

The timeline of a digital forensics project varies greatly based on the case complexity, data volume, available resources, and legal requirements. While some cases may be resolved in days or weeks, others, particularly complex ones, may take months or longer. The key is balancing thoroughness and accuracy with timeliness.