# CYBERSECURITY AUDIT

**CYBER EXPERTS & PENTESTERS**

**ON SITE OR REMOTELY**

**AUDITS & PENTESTS**

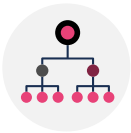
**ISO 27001 & 27002 CERTIFICATION - PCI DSS, GDPR & HIPAA**

## A LARGE CHOICE OF SECURITY AUDITS

Our team of cybersecurity experts helps you comply with PCI DSS, GDPR & HIPAA by realizing custom-made audits according to your project. They also help you achieve ISO 27001 and ISO 27002 certification by offering cybersecurity audits modules designed for these standards.

ziwit
Consultancy Services

# YOUR COMPANY OVERALL



## ORGANIZATION AUDIT

Analysis of your entire organization and of its level of security. Not only your security policy and your security procedures are audited but also the security strength of your IS.

*For the purpose of ISO 27001/27002, SMSI certifications*

## REDTEAM SERVICES

Penetration test performed against your organization as a hacker might do. The pentester has no perimeter limit. He is to exploit all the possibilities of technical (Network scan, applicative scan, penetration test, priviledge escalation, dataleak, Active Directory...) and non-technical attacks (Social Engineering, Recoveries, Infiltrations...).

## VIRTUALIZATION AUDIT

Analysis of the security level of the virtualization platform you use. Our team audits several points: hypervisors reinforcement, patch management, sealing between your virtual machines, segmentation of your virtual networks, admin accounts management, SAN security, admin process and more depending on your organization.

*Scope of the audit: VMware, vSphere, vCenter, XenDesktop, Hyper-V*

## AUDIT AD

Audit of your global architecture, not only the forests but also the domains. This audit aims to reinforce the domains controllers, the groups, sharing and accounts management and password strength.

*Scope of the audit: NTDS, GPO, NTLM, approval relationship...*

# YOUR DATA AND CLOUD ENVIRONMENT

## CLOUD INFRASTRUCTURE AUDIT: AWS/AZURE/GOOGLE CLOUD

Our team of cyber experts analyses the security level of your cloud environments, such as AWS, Azure or Google Cloud.

*Instance exploitation, access control, keys compromission, logs compromission, configuration audit...*

## DATA AUDIT

Audit of your entire data infrastructure. Your data collection, processing and storage system. The scope goes from the audit of your systems and applications to the audit of your entire data infrastructure administration.

*HDFS, ElasticSearch, Hadoop, Xen, RabbitMQ, Cloudera, LogStash, Kibana.*

# YOUR PHONE INFRASTRUCTURE, YOUR ERP AND YOUR MAIL SERVICES

## TOIP / VOIP AUDIT

We audit your entire IP based phone infrastructure: IPBX (Internet Protocol Private Branch eXchange), Virtual LAN, workstation, switches, taxation server, recorders and even more according to your organization.

*Communication systems such as Cisco, Avaya, Alcatel, NICE, SIP.*

## SAP AUDIT / ERP

As ERP software is used daily in your company, make it audited entirely to detect its vulnerabilities: not only the databases, the system, the network, the encryption, the application server, the accounts, the passwords but also GIU, batches, APIs.

## EXCHANGE / WEBMAIL AUDIT

Your mail is an entry point for hackers. To audit the configuration and the administration of your email service is crucial. Our experts realize complete audits: rights, passwords, patches, files, system, backup and existing protections (antivirus and antispam).

*Simple Mail Transfer Protocol SMTP, Outlook Web Access OWA, Microsoft Exchange and more depending on your organization.*

# YOUR PASSWORDS AND WORKSTATIONS MANAGEMENT

## PASSWORDS AUDIT

If you have a global security policy, we audit the degree of its application by setting up a precise measurement of: the proportion of weak passwords, useless accounts or services...

*Scope of audit including all types of technologies depending on your organization: LDAP, AD, applications and more.*

## WORKSTATIONS AUDIT

We audit restrictions, systems and applications patches, encryption, local passwords, scripts and installed programs. We make the most of the workstations audits to raise awareness among the user, as well as to install and to apply the correctives.

*Define your type of workstations: desktop, laptop, virtual office, tablet and more depending on your organization.*

# YOUR APPLICATIONS AND WEBSERVICES


## WEB APPLICATIONS, SAAS, CLOUD AUDIT

Your application system is a major entry point for hackers. We realize an audit of your application infrastructure, codes and application logic: access rights, hosting system, passwords, responsive functions, the forms, sessions, uploads, privilege escalation, inputs/outputs, but also data protection.

*Audits performed on Java, PHP, .NET, JS, Symfony, Zend, Spring, Struts, AWS, Azure and more depending on your organization.*


## WEB SERVICES / API AUDIT / (MOBILE APPLICATIONS / IOT)

Penetration test like a malicious hacker had an access to your Front and back-office API to detect the existing vulnerabilities.

*Audits performed on XML, SOAP, JSON, Ajax, REST.*


## CODE AUDIT

Your source code is fully audited to detect security flaws, bugs or vulnerabilities. We perform an audit which combines a traditional review of the static code and "in vivo" security tests on a test environment.

*Flaws detection, Code review, OWASP, CWE, PCI DSS.*

# YOUR OPERATING SYSTEM

## WINDOWS SYSTEM AUDIT

Administration process analysis of your Windows systems and their configurations. Our experts audit your systems with reference to your PCI DSS best practices policy.

*Session, rights and passwords management; System hardening; Patch management; Group Policy.*

## LINUX SYSTEM AUDIT

Administration process analysis of your Linux systems and their configurations. Our experts audit your systems with reference to the reinforcement guidelines for distribution such as Redhat, CentOs, Debian, Suse or Oracle. Our team analyses also the configuration of available services such as Apache, Tomcat, Jboss ...

*System hardening; Patch management; rights management; passwords management.*

# YOUR INFRASTRUCTURE

## INFRASTRUCTURE AUDIT AND EXTERNAL EXPOSURE

The audit is performed on your networks components, your systems and your infrastructure service to detect the vulnerabilities that hackers could exploit.

*Scope of the audit: VPN, firewalls, Web servers, DNS, Reverse-proxy, FTP, SMTP...*

## INTERNAL NETWORK / LAN AUDIT

The audit starts with a connection to your LAN as an employee or a visitor might do. Then, we look for all the flaws allowing to access to sensitive data and to gain privileged administration rights on the IS.

*Network security, vulnerability scanner, mapping, exploitation, attacks.*

## INDUSTRIAL SYSTEMS AUDIT

Analysis and audit of your industrial systems, networks, access points and the different ingoing/outgoing communications.

*Management of obsolete protocols on sensitive business systems: S7, Modbus, VACnet, RS, DNPR, ...*

ziwit
Consultancy Services

## A NEED FOR A CYBERSECURITY AUDIT? CONTACT-US!

**+33 1 85 09 15 09**
**WWW.ZIWIT.COM**


**MONTPELLIER**
40 Avenue Théroigne de Méricourt
34000 Montpellier
France

**PARIS**
84 Avenue du Général Leclerc
92100 Boulogne-Billancourt
France