www.spearit.net

ABOUT US

SpearIT is dedicated to providing guidance over enterprise governance of information technology, subject-matter expertise as well as enabling visibility and promoting continuous improvement of cyber security in evolving markets and industries, especially where standardization is loose and complexity is high.

Our services portfolio ranges from cybersecurity assessments, security operations to holistic Enterprise Governance of Information and Technology, Enterprise Architecture, Risk, Compliance and IT Service Management for organizations in emerging industry sectors, such as Trust Services and Electronic Identification, Technology Service Providers, Critical National Infrastructure and Governmental Authorities. Our subject matter experts team is actively involved in various working groups and committees, contributing to the development of some of the most evolving digital trust and cyber security standards in EU and US.

CISSP Certified Information Systems Security Professional · CISM Certified Information Security Manager. An ISACA Certification · ISO 27001 Lead Auditor · ISO 27001 Lead Implementer · CCSK Certificate of Cloud Security Knowledge · OSCP Offensive Security · COBIT 2019 · ITIL · PRINCE2

Equitable Solutions

We maintain an independent mindset and solid approach, not influenced by product sales interests. Thus, your organization is assured it receives an unbiased, tailor-made and cost-effective final solution.

360-degree Reporting

Having a multidisciplinary team with experience in both technical and managerial positions, we are capable of speaking a multidimensional language to cover all aspects of your organization, delivering the proper message to the proper audience in a clear and effective way.

Passion and Discipline

Curiosity is our passion, continuous improvement our discipline. Achieving the balance of these two forces, allows us to deliver projects with the highest quality and at the same time, expand our peoples' skill set and knowledge.

INDUSTRIES & SERVICES OVERVIEW

Our cybersecurity solutions cover a wide range of emerging industry families and support your organization's cybersecurity journey from assessment and security testing services to holistic consulting and compliance services.

INDUSTRIES

DIGITAL TRUST

- eID & IdPs
- Trust Service Providers

TECHNOLOGY SERVICE PROVIDERS

- ISPs
- Datacenters
- Cloud services
- Software houses

OPERATORS OF ESSENTIAL SERVICES

- Energy
- Transport
- Drinking water supply
- Digital infrastructure
- Healthcare
- Banking

GOV/EU AGENCIES

- EU decentralized agencies
- National governmental authorities

CISOaaS

CYBERSECURITY ASSESSMENTS

IT COMPLIANCE

SERVICES

Discover our Service Portfolio

CISOaaS

Aligned with **EU NIS2 Directive**

Contrary to a traditional CISO role, **CISOaaS** is based on a multidisciplinary team of cybersecurity professionals with perennial experience in regulatory compliance and consulting on 360-degree cybersecurity domains coverage, delivering customized services remotely and/or on-site based on your particular needs, achieving significant cost reduction.

OUR APPROACH

1. SCOPING

Based on your organization's type of operations, infrastructure and risk appetite, an assessment is performed to identify the regulatory, legislative and contractual requirements that the organization must meet.

2. GAP ANALYSIS

A gap analysis is conducted to identify what needs to be protected and at what level. The general security strategy is developed and the particular service characteristics are identified along with the service delivery time plan.

3. INITIAL IMPLEMENTATION

The initial implementation roadmap is followed, providing the deliverables of each phase and reaching the milestones set by the management board.

4. CONTINUOUS MAINTENANCE

Continuous monitoring of the roadmap by establishing and executing day-to-day business activities on the agreed-upon time basis. Reporting to upper management levels and planning of compensating actions sets a constant force of improvement, minimizing costs, risks and administrative overhead while maximizing your organization's cybersecurity posture.

SERVICE PROVISIONS

- Planning & implementation of the security policy documents, procedures, documentation management and maintenance
- Self-assessment procedures and reporting to national entities
- Risk identification, assessment and treatment
- Support in new systems deployment under the aspect of cybersecurity
- Supply chain and SLA assessments
- Design and deployment of staff cybersecurity awareness training
- Incident management and response
- Support in IT security solutions procurement
- Organization's point of contact among upper management & national bodies (e.g. CSIRTs, National Cybersecurity Authorities)

KEY BENEFITS

Ensured Compliance

Become and stay compliant eliminating the administrative hassle of regulatory requirements.

Continuous Improvement

Ensure continuous monitoring of your organization's security level in order to continuously minimize risks and improve your security posture.

Cost Reduction

Achieve reduction of you cybersecurity expenses via choosing balanced and proper IT solutions.

Damage Avoidance

Avoid non-conformity penalties and minimize the financial and reputational damage of your organization by following a holistic, strong and solid security program.

PKI & TSP CONSULTING

Digital certificates meet a continuously growing demand by enterprises and national organizations. Electronic identification (eID), seamless cross-border transactions, zero-trust models are some of the modern and evolving cases of trust services importance.

SPEARIT Public Key Infrastructure (PKI) Consulting Services help you:

- ✔ Design & deploy self-managed PKIs according to your business needs.
- ✔ Stay compliant against trust service regulations & standards.
- ✔ Achieve inclusion in root store programs and become publicly trusted CAs.

STANDARDS & REGULATIONS COVERAGE

- ✔ **ETSI**
- ✔ **eIDAS**
- ✔ **CAB/F BR, NSR, CS, EVCG**
- ✔ **WebTrust**
- ✔ **Browser Root Programs**

Policies & Documentation

Planning & guidance on documentation requirements:

- Certificate Policy (CP)
- Certificate Practice Statement (CPS)
- Validation Plan
- PKI Hierarchy

Certificate Profiles Audit

Certificate profiles compliance audit against:

- ETSI requirements
- CAB/F BR
- EVCG
- CS
- Root Stores

PKI Critical Assets Audit

Compliance audit of the critical components of your PKI system:

- Root CA
- Sub CAs
- Certificate sampling
- OCSP Responders
- CRLs

Technical Consulting

Consulting & compliance on:

- Trusted roles management
- Access control
- Monitoring & reporting
- Disaster Recovery
- Vulnerability Remediation
- Risk Management

Cyber Security Assessments

Vulnerability Scanning
Penetration Testing

REMOTE KEY ATTESTATION

Certificate Authorities traditionally perform in-house the witnessing of remote key material generation inside the customers' FIPS compliant infrastructure, pertaining to EV code signing & document signing certificates. This usually accretes the total cost of EVCS, document signing and cloud signing certificates. By delegating the witnessing procedure to a trusted external entity, issuing CAs achieve a reduction of the total time required for issuing these types of certificates which translates to a **reduced cost**.

Technical Competency

Our solid technical background & understanding of encryption and key management operations ensures that the key attestation procedure is meticulously audited, eliminating false opinions which may dictate the revocation of your keys at a later time.

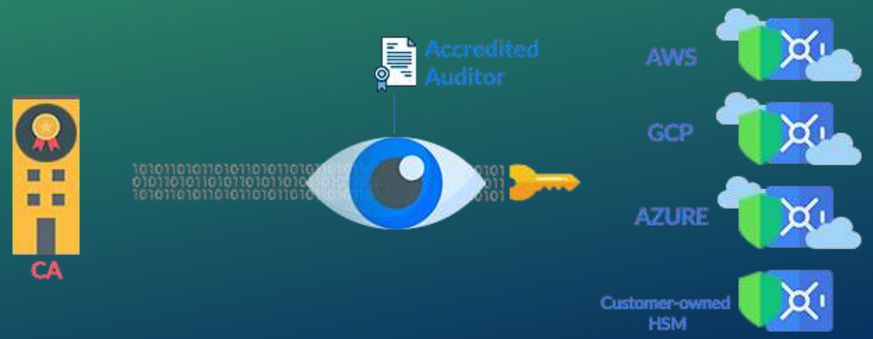
Auditing Competency

Always staying in-line with the latest regulatory and compliance developments, our PKI auditors hold well-respected accreditations and certifications related to PKI & cloud security auditing, ensuring a firm understanding of the compliance domain related to EV code signing and AATL document signing.

Code of Ethics

Adherence to the standard code of ethics of the relative certification or accreditation our auditors hold, ensures the highest quality, transparency and impartiality of the offered service, validated by respected standardization organizations, such as ISO/IEC and ETSI.

ACCREDITED ATTESTATION PROCEDURE



By leveraging our team of accredited PKI auditors, a real-time observation of the key material generation procedure is performed, ensuring that the appropriate controls and procedures were applied from key generation to key storage. At the end of the witnessing procedure, we provide you with a signed attestation letter regarding the proper generation of key material inside your FIPS compliant device, located on-premises or on cloud.

aws Azure Google Cloud

utimaco® THALES ENTRUST

CYBER SECURITY ASSESSMENTS

Security assessments rely on three main assessment methods that are inter-related: Technology, People and Processes. Our assessments are tailored to your company's environment and needs, assessing specific aspects of your security program.

Assessment Type	Scope	Objective	Benefit
Vulnerability Scanning	Internal / External	**Identify known & published vulnerabilities on systems & software used inside your company.**	**Understand your attack surface characteristics and easily plan mitigation actions to minimize the impact of a security breach**
Infrastructure Penetration Test	Internal / External	**Identify and exploit vulnerabilities on systems, services and applications exposed to the Internet or Intranet**	**Understand and minimize business risk from an internal or external breach**
Web-Application Penetration Test	Internal / External	**Assess web applications for vulnerabilities which lead to unauthorized access or data exposure**	**Understand and minimize business risk from a breach through web assets and critical data exposure.**
IoT & SCADA Penetration Test	Internal	**Assess the security of your smart devices and critical ICS/SCADA systems by attempting to exploit the embedded firmware, hijack management tools and finally control the device**	**Understand the security of smart devices and control systems and the ability before a real adversary exploitation happens**
Social Engineering Attack	N/A	**Assess the security awareness of your staff and general security controls through human manipulation**	**Measure your staff security readiness & understand the criticality of human factor in cyber security**
Cloud Security Assessment	N/A	**Detect & mitigate common cloud environments misconfiguration, minimize attack landscape**	**Understand the threats and security controls unique to your specific cloud environment**
Red Team Exercise	N/A	**Test the overall security readiness of your organization, including staff, procedures, facilities & technical controls**	**Raise security awareness, identify gaps in your cyber security program**

Deliverables

- Multi-level reporting for the various organizational departments
- Mitigation recommendations
- Risk contextualization to confirm a critical finding is relevant to the targeted environment
- InfoSec Certificate & SpearBadge™ continuous improvement indicators

For a detailed view on each cyber assessment service, visit https://www.spearit.net/services/security-assessments

VULNERABILITY SCANNING

Vulnerability scanning is usually preferred as a first step in discovering flaws in the security of systems. A **quick, non-invasive, non-disrupting** security assessment process which utilizes a highly detailed and regularly updated database of vulnerabilities, able to detect ✔ **configuration issues** ✔ **missing patches** ✔ **published vendor vulnerabilities**.

SPEARIT offers a "2-lane" vulnerability scanning service to match your various security needs:

STANDARD VERSION

- Quick overview of vulnerabilities
- Basic insight in security status
- Security Planning of early system development

★ Standard Recommendations

★ Scheduled Scanning

★ Detailed Technical Report

Intensity

COMPLIANCE VERSION

- Periodic monitoring of vulnerabilities
- Complete vulnerability management
- Mission-critical systems
- Compliance scanning criteria

★ Detailed Recommendations

★ Vulnerability Notification SLA

★ Incremental Reporting

★ Detailed Technical Report

★ Mitigation Verification

★ Context-aware scoring

Intensity

For a detailed view on vulnerability scanning services, visit https://www.spearit.net/services/vulnerability-scanning

PENETRATION TESTING SERVICES

Designed to provide high quality insights for the various organizational domains, our penetration testing covers a wide range of business or security needs. The actual testing methodology consists of commercial and proprietary tools, guided by well-known penetration testing standards and enriched with manual and hybrid testing methods.

OUR APPROACH

1. SCOPING
An operational environment is discussed and established with the help of written/verbal communication & scoping questionnaires, defining the characteristic of the engagement.

2. INFORMATION GATHERING
Passive OSINT (Open Source Intelligence) techniques are used in combination with neutral observation actions in order to collect as much information as possible regarding the targets to be tested. The more the information collected, the most attack vectors can be crafted.

3. ENUMERATION
A plethora of automated tools and manual scanning methods is utilized in order to discover possible entry points and attack vectors.

4. EXPLOITATION
Based on the findings of the previous steps, proper attack vectors are designed and executed in order to exploit the detected vulnerabilities/flaws and penetrate into the application.

5. REPORTING
Reports are a crucial step in a penetration testing engagement as the cornerstone deliverable which provide meaningful insights regarding the security posture of your organization, along with remediation recommendation for each detected risk.

6. MITIGATION VERIFICATION
The verification procedure aims to approve the proper implementation of the proposed mitigation measures and to detect any new vulnerability which may arise from the reconfiguration activities which would probably occur in the context of mitigation.

FOCUS AREAS

Infrastructure

- External IP blocks and relation to hosting providers
- Domains and subdomains
- Leaked credentials
- Publicly exposed systems
- Misconfigured DNS & web servers leaking information
- Open ports & services
- Services misconfiguration
- Network & Application Firewall fuzzing
- Network segmentation testing
- MitM attacks
- Known vulnerabilities (CVE, CVSS, etc.)
- Exploitation of known service vulnerabilities
- Breached/brute-forced credentials usage
- Information exfiltration and lateral movement
- Privilege Escalation attacks
- Active Directory attacks
- Lateral movement

Web-Application

- Leaked document and other file types by various search engines
- Exposed robots.txt file
- Past credential leaks
- Forum posts by developers
- Directories/subdomains enumeration
- Services misconfiguration
- Exposed backup/config files
- Known vulnerabilities (CVE, CVSS, etc.)
- Authentication Mechanisms
- Session Handling
- Input Validation
- Code Injection
- Request Forgery
- Encryption Mechanisms
- Services Misconfiguration (web/database/FTP/DNS/email, etc.)
- Information Disclosure Issues
- Software Versions
- Service Availability (DoS)
- API testing

IoT & SCADA

Alignment with **OWASP IoT Project**

- Application binaries reverse engineering
- Firmware binaries reverse engineering
- Encryption & obfuscation techniques analysis
- Used 3rd party libraries analysis
- Assessing hardware communication protocols
- Tampering protection mechanisms
- Fuzzing & side-Channel attacks
- Assessment & exploitation of wireless protocols
- Attacking protocol specific vulnerabilities
- Web application & API (hosted or cloud) vulnerability exploitation
- Desktop application vulnerability exploitation

Deliverables

- Multi-level reporting for the various organizational departments
- Express mitigation recommendations
- Long-term recommendations to transform your current security posture
- Mitigation verification to ensure proper technical implementation

For a comprehensive view of the various penetration testing services, visit our cyber security assessments page at **https://www.spearit.net/services/security-assessments**

SOCIAL ENGINEERING ATTACKS

Assess the security readiness of people by crafting attack scenarios against staff or suppliers.

OUR APPROACH

1. SCOPING
An operational environment is discussed, defining the characteristics of the engagement, objectives, targets, attack scenarios and types.

2. INFORMATION GATHERING
Passive and active OSINT (Open Source Intelligence) techniques are used in order to collect valuable social information.

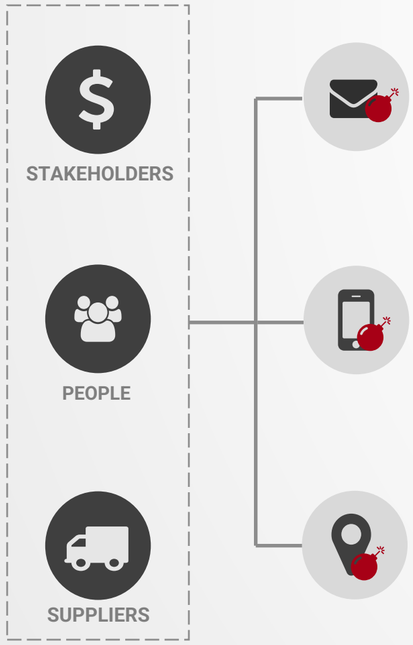
3. PAYLOAD CRAFTING
Based on the information gained from the previous step, the phishing payloads are crafted, targeting a set of people, combining real facts regarding each target, in order to be as realistic as possible.

4. ATTACK
The actual attack starts here, with carefully crafted emails & landing pages, voice calls & AI voice mimicking, exploiting the human targets according to the objectives.

5. REPORTING
When the phishing campaign completes, a **risk-based report** is generated including an executive and technical report, success ratio, statistics per department and improvement recommendations.

6. AWARENESS TRAINING
Optional offer training services for your personnel, in order to establish or maximize the already established security awareness withing the team. The training can either target specific employees/departments or be offered in a more systematic way to your internal compliance officer/security department in order to integrate awareness to your company's security policy.

ATTACK TYPES & TARGETS



EMAIL

Spoofed emails with malicious payloads are crafted in order to exploit human targets via client-side attacks. Payloads include:

- Malicious HTTP links
- XSS, CSRF, Session hijacking techniques
- Attachments targeting specific client-side OS vulnerabilities

VOICE

Phone phishing attacks (VISHING) aim to exfiltrate sensitive information over the phone by manipulating the victim to carry out specific actions.

PHYSICAL

Attacks carried out in the organization’s physical site, either by co-operation with delegated employees or impersonation of a trusted identity.

AT A GLANCE

A simulated attack from the perspective of a malicious actor.
The objective is to exfiltrate sensitive information by combining manipulation of human factor through social interaction (email, phone, in-person) and technical exploitation of vulnerabilities.

BENEFITS

- Assess the security readiness of your staff
- Identify gaps in your cybersecurity awareness program
- Design better & more effective trainings

Humans are the most crucial factor in the cyber security chain!

For a comprehensive view on social engineering, visit
https://www.spearit.net/services/social-engineering

CLOUD SECURITY ASSESSMENTS

Identify, understand and mitigate gaps and weaknesses in your cloud environment. Gain visibility and granular control over attacks. Our cloud security engineers perform a thorough review of your security model and governing policies as well as specific security configuration, leveraging vendor-specific security features of your platform(s).

OUR APPROACH

PHASE 1

Documentation Review:
Review and assessment of your cloud architecture diagrams, access management policies, security policies, monitoring & logging policies, disaster recovery policies.

PHASE 2

Onsite Assessment:
Your cloud infrastructure is hands-on examined by our cloud engineers, reviewing your current security model and everyday management operations to identify gaps or improvement areas.

PHASE 3

Configuration Review:
Your cloud platform configuration is reviewed to ensure security controls are implemented effectively, identify potential weaknesses and propose possible improvements.

PHASE 4

Final Reporting:
Risk-based report depicting strong & weak areas, along with specific improvement actions in order to strengthen your cloud environment security posture and enhance visibility and threat response capabilities of your security team.

Focus Areas

Governance, Risk & Compliance
- Cloud policies & standards
- Regulatory compliance
- Risk Assessments
- Vulnerability Management
- Penetration Testing

Cryptography
- Certificate Lifecycle Management
- Encryption
- Password Management

Security Architecture
- Cloud Security Architecture
- Network Segmentation
- On-premises interconnection
- Disaster Recovery

Access Control
- IAM
- RBAC
- ADFS
- 2FA mechanisms

Threat Detection
- Logging & Monitoring
- Edge Network Security
- Endpoint Network Security

DevOps
- SSDLC
- Code Repo Security
- Application Deployment & Decommission
- System Deployment & Decommission

Deliverables

- Multi-level reporting for the various organizational departments
- Recommendations for enhancing visibility and security
- Long-term recommendations to transform your current security posture

PROVIDER COVERAGE

Azure · amazon web services · Google Cloud Platform

SERVICE MODEL COVERAGE

✔ IaaS ✔ PaaS

For more information, visit
https://www.spearit.net/services/cs-assessments

RED TEAM EXERCISES

Full-range and complex assessments for mature technical & security teams, simulating the behavior of an external adversary against your organization. Our red team mimics a real adversary's attacks by using tactics, techniques and procedures as seen on real cases, ranging from physical & perimeter security to actual exploitation and threat persistence.

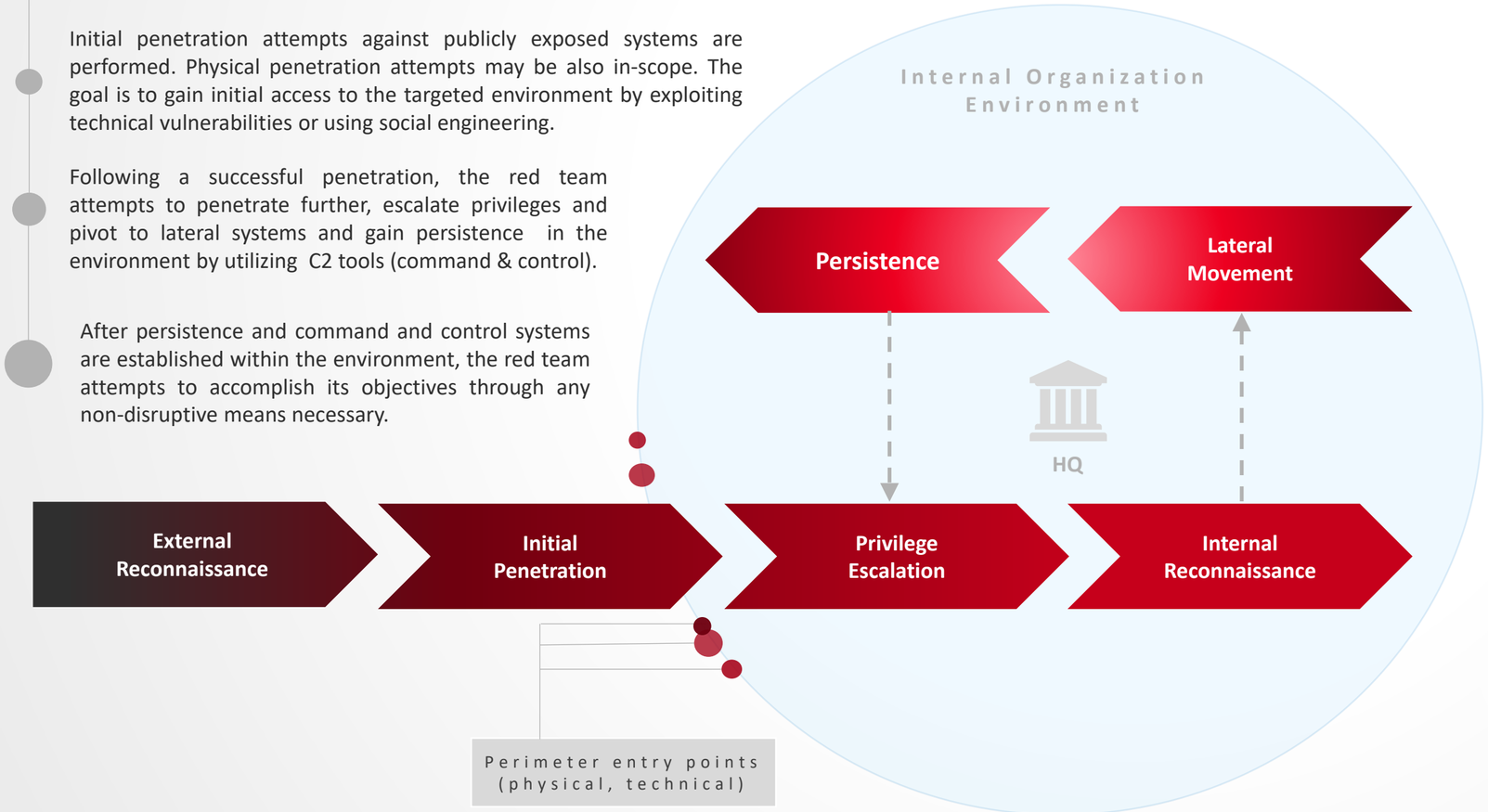
OUR APPROACH

The operation starts with the initial reconnaissance phase. A combination of various intelligence sources and methods is utilized to collect information which allows the red team to design proper attack vectors.

Initial penetration attempts against publicly exposed systems are performed. Physical penetration attempts may be also in-scope. The goal is to gain initial access to the targeted environment by exploiting technical vulnerabilities or using social engineering.

Following a successful penetration, the red team attempts to penetrate further, escalate privileges and pivot to lateral systems and gain persistence in the environment by utilizing C2 tools (command & control).

After persistence and command and control systems are established within the environment, the red team attempts to accomplish its objectives through any non-disruptive means necessary.



BENEFITS

- Identify and mitigate security vulnerabilities in your infrastructure
- Identify and repair weaknesses in your security program and security plan
- Measure your team's threat detection and response levels
- Risk-based reporting and recommendations for improving your security posture
- Maximize awareness of your staff, vendors and stakeholders

For a comprehensive view on read team attacks, visit
https://www.spearit.net/services/redteam-attacks

IT COMPLIANCE

Our method breaks down in **five** major phases:

The appropriate documentation (incl. policies, procedures, manuals) are implemented according to your organizational and operational environment needs.
Designed in a smart way to minimize the administrational effort and stay maintainable throughout the years.

SPEARIT trains your employees to become familiar with the newly developed management system, targeting the various organizational departments (executives, marketing, sales, technical, administrative). The final goal is for everyone to become familiar with the "new way" your company will operate.

A pre-certification audit is carried out by specialized in auditing procedures **SPEARIT** staff. The goal of this process is to simulate the final certification, in order to detect and correct any non-conformances but also, make your company's employees feel a little more relaxed as they witness a real auditing scenario where they are actually asked for various evidence. This way, they become more confident during the final auditing procedure by the accredited certification body.

The official audit process is carried out by an accredited certification body.
Certified auditors will visit your company's location and perform various inspections regarding the documentation and the implementation. Upon complete inspection which usually lasts a couple of days, the certification body issues your certificate or informs you about additional actions you shall carry out in order to receive the certificate of compliance.

SPEARIT continuously oversees your compliance status by

- performing recurring technical assessments (vulnerability scans, penetration tests)
- consulting with key personnel regarding maintenance and improvement of your management system
- proposing compensating controls/improvement actions

Our perennial expertise in implementing and auditing Information Security Management Systems lets us guide you with a smart way in choosing the appropriate implementation and provide you with extra consultancy in various areas.

ISO/IEC 27001:2013
ISO/IEC 27017:2015
ISO/IEC 27018:2019
ISO/IEC 20000:2011
ISO/IEC 22301:2019
GDPR EU 2016/679
NIS2 Directive 2016/1148
(EC) No. 2018/1725

In cases where a certification is needed, our smart certification approach takes you there, worry-free and with the minimal administrational effort!

Interested in becoming compliant? Visit

https://www.spearit.net/services/it-compliance

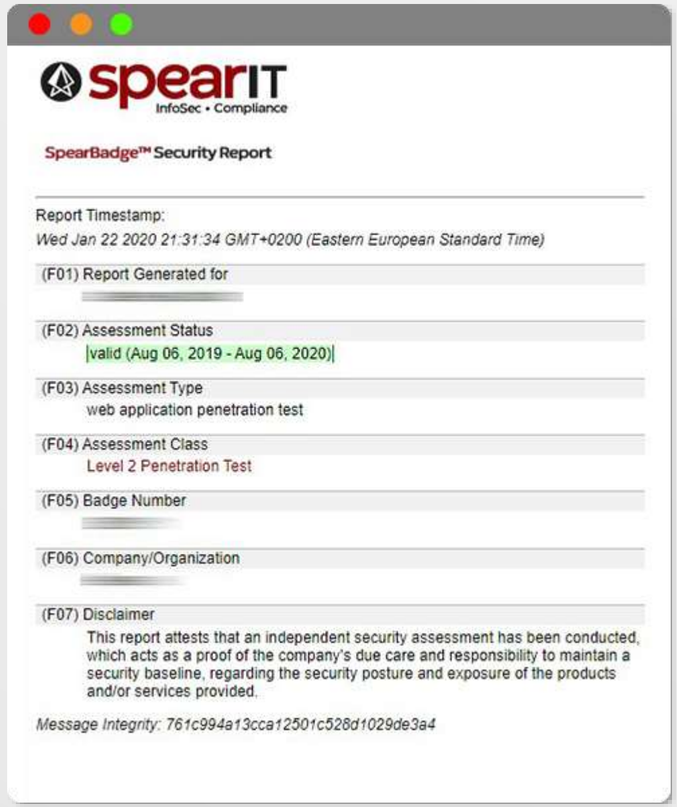
SPEARBADGE™

SpearBadge™ is an ad-hoc service that establishes trust by declaring your product's security readiness and your due diligence to maintain a security baseline. It applies to any security assessment service conducted.

Displaying the **SpearBadge**™ in your site, is letting your customers not only know that your organization values security, but that you continuously maintain and improve your security level.

The logo consists of 3 informational elements:

- **Certification Class**: level of assessment the organization has passed. The higher the level, the more exhaustive and detailed the security assessment.
- **Domain of Certification**: type of assets assessed (networks, web apps, infrastructure).
- **Certificate Number**: unique number that identifies the assessed organization and can be used in our lookup tool to verify the organization's trust.


spearIT
InfoSec • Compliance

SpearBadge™ Security Report

Report Timestamp:
Wed Jan 22 2020 21:31:34 GMT+0200 (Eastern European Standard Time)

(F01) Report Generated for

(F02) Assessment Status
valid (Aug 06, 2019 - Aug 06, 2020)

(F03) Assessment Type
web application penetration test

(F04) Assessment Class
Level 2 Penetration Test

(F05) Badge Number

(F06) Company/Organization

(F07) Disclaimer
This report attests that an independent security assessment has been conducted, which acts as a proof of the company's due care and responsibility to maintain a security baseline, regarding the security posture and exposure of the products and/or services provided.

Message Integrity: 761c994a13cca12501c528d1029de3a4

When a visitor clicks on the **SpearBadge**™ logo, a real-time report displays status information about your organization and your products security assessment.

General Information
info@spearit.net

Sales Department
sales@spearit.net

+30 2311 320 270

Egnatia 154
Thessaloniki 54636
GREECE

+372 60 28 548

Tornimäe 5
Tallinn 10145
ESTONIA

Official Website