SERVICES CARD

baysec.

https://baysec.eu

Table of Contents

Services

Below we present a set of services developed with comprehensive organizational protection against modern cyberattacks in mind.

1. Red Teaming and Penetration Testing

Red Team Assessments – Adversary Emulation

We execute **advanced attack scenarios** that mirror the activities of real cybercriminal groups to test organizational resilience against the most sophisticated threats.

- **Advanced attack simulation** using techniques, tactics, and procedures (TTPs) of specified or unspecified adversaries.
- **Full attack chain emulation:** from initial access (e.g., spear-phishing, 0-day exploits), through environment persistence, lateral movement and privilege escalation, to objective realization (e.g., data theft, ransomware).
- **Intelligence integration (CTI)** to mirror real, most probable attack scenarios.
- **Security effectiveness evaluation** and assessment of defensive teams detection and response capabilities.
- Actions comply with the **MITRE ATT&CK framework** – final report includes technique mapping, detection effectiveness assessment, and security recommendations.

Penetration Testing

- **Security gap identification** in systems, applications, and networks.
- **Detailed reporting** with test results containing evidence, threat prioritization, and remediation recommendations.
- **Risk assessment** and potential impact evaluation of discovered vulnerabilities on the client environment.

Web Application Penetration Testing

- We conduct **comprehensive web application pentests**, identifying vulnerabilities.
- We analyze application business logic, configuration errors, resource availability, and potential attack vectors.
- We deliver detailed reports with risk levels, proof of concept (PoC), and specific remediation recommendations.

Active Directory Penetration Testing

- We verify **Active Directory environment security**: from incorrect GPO configurations, through Kerberos vulnerabilities (e.g., Pass-the-Hash, Kerberoasting), to privilege escalation.
- We **simulate realistic attack scenarios**, assessing infrastructure resilience to compromise.

AI Penetration Testing

- We conduct **comprehensive security assessment** of AI/ML/LLM systems used in organizations.
- **We identify model vulnerabilities** to popular attacks.
- **We test model resilience** to manipulation, abuse, and other forms of security threats.

Phishing Analysis

- We **investigate phishing campaigns** targeting the organization. We analyze malicious links, domains, and attachments. We identify attack sources and assess security effectiveness and user awareness.
- Upon request, we also conduct **simulated phishing campaigns** that allow assessment of employee readiness and organizational response effectiveness.

Physical Red Teaming/Social Engineering Tests

We conduct controlled tests involving **physical attempts to gain access to organizational resources** to assess resilience to social engineering threats and procedural errors:

- We simulate real attack scenarios (e.g., impersonating employees, couriers, service technicians) to assess personnel alertness levels and access control procedure effectiveness.
- We verify the possibility of gaining **unauthorized access to offices, equipment, documents, or systems** using social engineering techniques and physical security bypass.
- We report identified weak points and provide recommendations regarding training, security procedures, and physical security.

2. Risk & Vulnerability Assessments

- **Risk analysis**: impact and probability assessment of security gap occurrence.
- **Mitigation recommendations**: creating dedicated incident response plans and defense-strengthening strategies.
- **Clear reports** with prioritization and remedial action descriptions.

3. Malware Analysis & Reverse Engineering

- **Deep malware analysis** enabling understanding of behavior, attack vectors, and cybercriminal objectives.
- **Reverse Engineering**: breaking down samples into component parts to discover mechanisms, sources, and potential threat modifications.
- **Intelligence data integration (CTI)**: identifying attack indicators (IoC) and threat context, enabling faster response and protection.
- **Reporting:** delivering detailed analyses, conclusions, and defense strategy recommendations.

4. Courses and Training

- **Cybersecurity Training Adapted to Real Threats:** We conduct practical training for companies and institutions, covering strong password policy creation, popular attacks, and incident response. We teach through experience, using real examples and current threats.
- **Building Security Awareness and Culture in Organizations:** We help shape employee habits and attitudes that support cybersecurity. Training is conducted in an accessible manner, aiming not only to transfer knowledge but also to increase vigilance and responsibility in daily work.

5. Business Intelligence / Brand Intelligence

We offer comprehensive analytical services supporting business development and brand building, based on sales and marketing data.

- **Google Analytics integration and custom BI panels** – we connect analytical tools (GA4, Pixel, tags) and create dedicated analytical panels and reports compliant with individual business requirements.
- **Registry document verification** of specified companies.
- **Complete company verification** allowing information acquisition about business credibility and reliability. Includes company assets and information about debt or insolvency.
- **Intelligence covering company reconnaissance** illustrating its entire operations. This includes information about contractors, development plans, employment, and personnel. Premium business intelligence is dedicated to companies wanting to determine operational principles and main success sources of competition.
- **Personnel intelligence** – building networks of company management, personnel, and potential collaborators. This enables recognition of whether people we intend to cooperate with are trustworthy and whether cooperation involves risks.
- **Unfair competition intelligence covering investigation** and evidence material preparation regarding unfair competition activities such as impersonation, customer theft, customer persuasion to leave, or product imitation in digital environments.
- **Brand visibility and reputation analysis online** – we measure advertising campaign effectiveness, identify channels with the highest return, monitor opinions, and help remove false comments from portals and social media.

6. CYBER THREAT INTELLIGENCE (CTI)

THREATRIPPER PLATFORM

THREATRIPPER is a **modern cyber threat intelligence platform** supporting organizations in detecting cyber threats, vulnerabilities, and data breaches. It combines data from various sources to provide practical information enabling rapid response and effective risk management.

The system consists of three main components that functionally complement each other and form a cohesive whole:

VULNRIPPER – Vulnerability Inventory and Analysis

Vulnripper enables detection of vulnerable elements in IT environments and provides ready information allowing rapid risk reduction.

- Agents available for **Windows, macOS, and Linux systems** collect data about installed software and versions.
- The system automatically compares this data with known vulnerability databases (CVE).
- For detected vulnerabilities, related **exploits** are also presented if publicly available – enabling understanding of threat scale and action urgency.
- Vulnripper helps establish action priorities by showing which vulnerabilities are actually used in attacks or can be easily automated.
- The entire process occurs without external system integration requirements, making the solution quick and easy to implement.

OSINT – Open Source Intelligence

OSINT module handles automatic monitoring and analysis of publicly available information about cyber threats.

- Internet, forum, dark web, social media, and pastebin searches.
- Identification of mentions about new attack techniques, tools, APT groups, and industry incidents.
- Result matching to organizational profile (technologies, sector, geolocation).
- Early warning about threats that may impact client operations.

BREACHRIPPER – Data Breach Monitoring

The Breachripper module **enables identification of cases** when organizational user data may have been disclosed online – unknowingly or as a result of an attack.

- Verification whether **email addresses, logins, and passwords** associated with the company appeared in data breaches.
- Analysis of sources containing data from security breaches, including dark web, pastebins, and forums.
- Information about potential account takeover threats and recommendations for next steps (e.g., password change, MFA).
- Function particularly important for protecting customer, employee, and collaborator data.

7. OSINT

OSINT Raport

We execute comprehensive **Open Source Intelligence (OSINT)** activities for organizational needs, focusing on risk identification, threats, and unauthorized information circulation.

- **We collect and analyze data from open sources** (including internet search engines, social media, public registries) to identify potential threats, data leaks, or hostile entity activities.
- Based on collected information, **we prepare detailed reports** consisting of executed action descriptions, found information presented as threat descriptions, and recommendations for company security improvement.

Advanced Intelligence Reports

We create detailed, custom reports for organizational needs, including:

- **Threat group profiling (Threat Actors)** – analysis of specific APT/cybercriminal group activities, their techniques, known targets, and frequency.
- **Vulnerability, campaign, and incident reports** – industry threat reviews, phishing campaign analysis, ransomware, zero-day, etc.

*Reports are created on demand and adapted to specific organizational and sector needs.

8. Analysis

Post-Breach Analysis

- In case of security breaches, **we conduct detailed post-breach investigations**. We identify attack vectors, compromise scope, attacker activities, and incident consequences.
- We also support **reporting processes and remedial measure implementation** according to best practices.

Code Review

- **Source code review** for errors, vulnerabilities, and code quality. The service allows problem detection before deployment, increasing application security and functionality.
- **The service includes specific improvement suggestions** such as performance improvements, refactoring, security improvements with justification of benefits for code quality and maintainability.

Software Analysis Used in the Company

- **Inventory and assessment of used software** for security and vulnerabilities. The service allows identification of risky, outdated, or unauthorized applications in organizational environments.
- **Recommendations** regarding updates, elimination, or replacement of currently used software.

9. AI CONSULTING

- **We help select appropriate AI solutions** adapted to your business needs.
- **We develop reports containing**: technological recommendations, profitability analysis, implementation plan, and estimated implementation costs.
- **We support the entire process:** from concept, through tool selection, to integration and development.

10. Cyber Newsletter

We offer a regular newsletter with updates and analyses from the cybersecurity world, adapted to your organizational needs:

- Review of major threats and incidents – regular summary containing: popular attacks, zero-day vulnerabilities, malware campaigns, data breaches.
- Recommendations and best practices – specific guidance on protecting organizations against current threats.
- Dedicated industry sections – e.g., for financial, medical, industrial sectors, or public administration.

*The newsletter can be prepared in PDF format, online file, or as an internal report, in English and/or Polish.