ENCODERSPRO

ENCODERSPRO Cybersecurity

Your Trusted Shield in the Digital Realm

CIN: U85499UP2023PTC186703

ENCODERSPRO

About ENCODERSPRO Cybersecurity Services

PENTORA (Penetration Testing & Enterprise Network Threat Observation & Response Assessment) a subsidiary of ENCODERSPRO provides comprehensive cybersecurity services, combining penetration testing with real-time threat observation and response.

6+

Years of industry experience Testers

25+

Businesses protecting worldwide

95%

Client retention rate

99.9%

Recovered data in security incidents

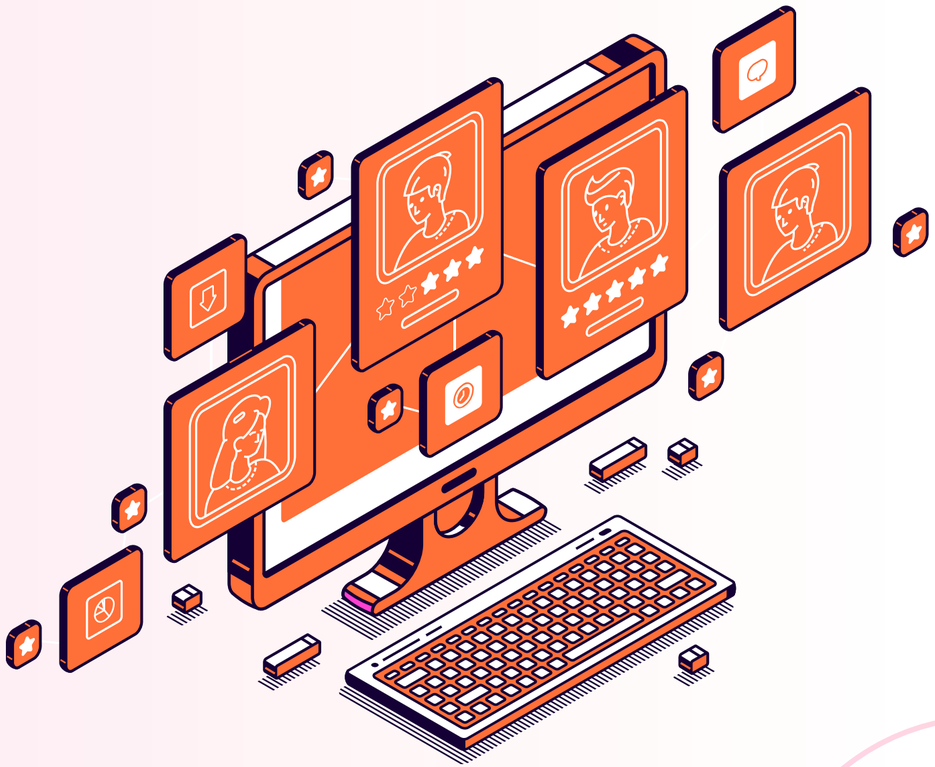
ENCODERSPRO

Tools & Technologies

Network Discovery & Mapping	Vulnerability Assessment	Exploitation & Validation	Password & Credential Testing	Configuration & Compliance Audits	Custom Testing Scripts
Nmap, Masscan, Netdiscover, etc	Nessus, OpenVAS, QualysGuard, etc	Metasploit Framework, Hydra, CrackMapExec, etc	John the Ripper, Hashcat, etc	CIS-CAT Pro, Lynis, HIPAA Security Rule Mapping	Python, Bash, PowerShell automation

ENCODERSPRO

Why choose ENCODERSPRO?



Most organizations lack the resources and diversified skills to find hidden vulnerabilities before attackers do. Unfortunately, using reactive tools alone leads to noisy, low-impact results that miss emerging risks.

- **24/7 threat monitoring**
- **Customized security solutions**
- **Deep expertise in cybersecurity**
- **Proven track record of safeguarding clients**
- **Certified Testers**

ENCODERSPRO

Our security services

ENCODERSPRO offers a wide range of cybersecurity services under PENTORA

Network Security

Customized solutions to prevent unauthorized access, monitor network activity.

VAPT Services

VAPT Services includes API Testing, Web Application Testing, Android Application Testing

Infrastructure Security

Secure infrastructure solutions to protect against external and internal threats.

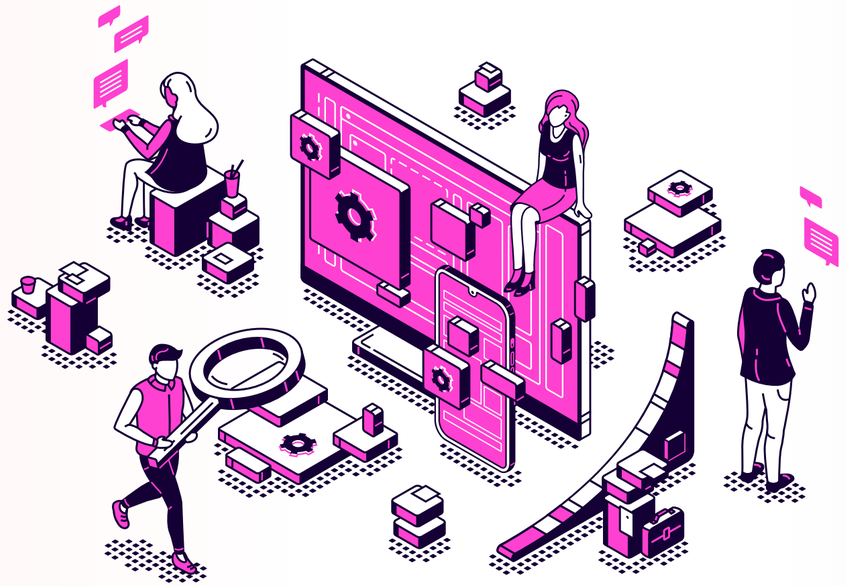
Cloud-native Security

Secure cloud environments to protect data and applications during migration and beyond.

ENCODERSPRO

Vulnerabilities Tested

List of vulnerabilities tested by PENTORA.



01.

OWASP TOP 10

The OWASP Top 10 is a list of the most critical security risks to web applications

02.

SANS 25

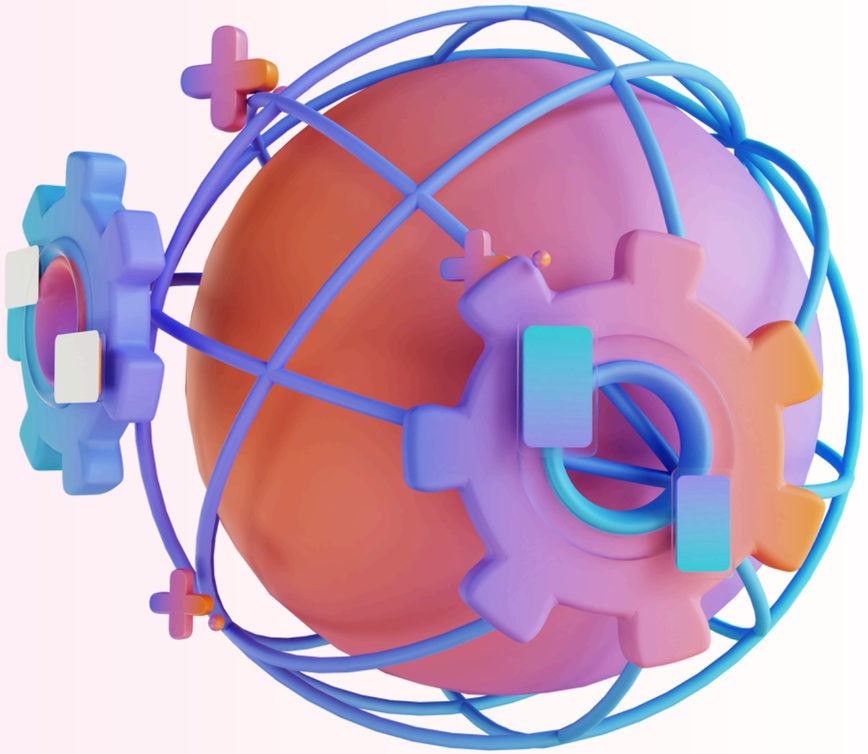
The SANS Top 25 is a list of the most common and dangerous software errors that can lead to security vulnerabilities.

03.

PTES

PTES stands for Penetration Testing Execution Standard.

Sentinel VAPT Methodology



At PENTORA, we introduce a groundbreaking approach called "**Sentinel VAPT Testing**." Unlike traditional VAPT providers, we go a step further by deploying our Web Application Firewall (WAF) agent on the client's servers (with their consent) during the assessment.

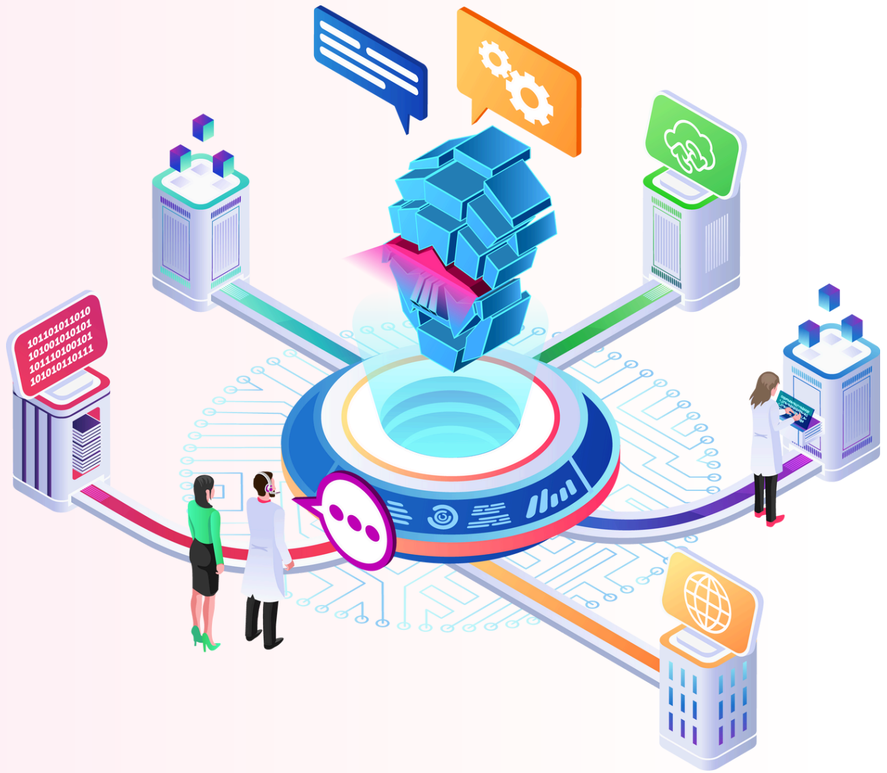
While our security experts manually test each endpoint, the WAF agent actively monitors real-time external attacks, logs incoming threats, and detects highly targeted endpoints. It also blocks injection payloads and identifies vulnerabilities based on live attack data.

This dual-layer approach enables us to prioritize critical security risks by combining real-time threat intelligence with hands-on penetration testing, ensuring comprehensive protection for our clients.

- **Dual-Layer Security Analysis**
- **Adaptive Threat Response**

ENCODERSPRO

Red Teaming Services



At PENTORA, we do **Red teaming** which is a realistic, controlled test where security experts act like real attackers to find weak spots in your systems, people, and processes. We try to break in, trick staff, and move through your network — all within agreed rules to keep things safe. The aim is not to blame anyone but to reveal real risks and give clear, prioritized fixes so your team and systems become stronger before a real attacker shows up.

The goal isn't to "catch people out" but to uncover practical gaps that could cause real business harm, then hand you clear, prioritized fixes so your SOC, incident playbooks, and leadership are better prepared. In short: red teaming shows you how an attacker would attack — so you can harden the places that matter most before anyone else finds them.

- **Simulate advanced persistent threats (APTs).**
- **Validate security controls end-to-end.**

ENCODERSPRO

Red Teaming Phases & Methodology

- **Pre-engagement & Planning** — Objectives, RoE, scoping, baseline data
- **Reconnaissance** — Passive & active OSINT, service discovery
- **Initial Access** — Phishing, credential stuffing, exploited public-facing apps
- **Privilege Escalation** — Exploit misconfigurations, credential harvesting
- **Lateral Movement** — Internal pivoting (RDP/SMB/AD abuse)
- **Objective Achievement** — Data exfiltration, persistence, business-impact demonstration
- **Post-engagement** — Reporting, remediation planning, retest

Aligned with MITRE Attack Framework.

AI based threat modelling reference.

Technical Depth: Tactics & Tools

- **OSINT & reconnaissance tools:** Shodan, Amass, hunter.io, custom scrapers
- **Exploitation & custom tooling:** Metasploit, Cobalt Strike (if allowed), custom scripts
- **AD & Windows techniques:** Kerberoasting, DCSync, Silver/Golden Ticket ideas (demonstration vs exploitation policy)
- **Linux & cloud techniques:** SSRF --> metadata abuse, IAM misconfigurations, container breakout checks
- **Network techniques:** Lateral movement via SMB, RDP, pass-the-hash, VPN pivot
- **Data exfiltration methods:** DNS tunneling, encrypted channels, cloud sync abuse

IoT Hardware/ Firmware VAPT

Web App & API Pentesting

Cloud-native Security

ENCODERSPRO

Protect your organization from attacks

We provides comprehensive network security services.

Mobile App Pentesting

Cyber Threat Intelligence

SIEM/XDR Deployment

Network Security Pentesting

Security Audit - ISMS, SOC, ISO 27001

ENCODERSPRO

ENCODERSPRO Methodologies

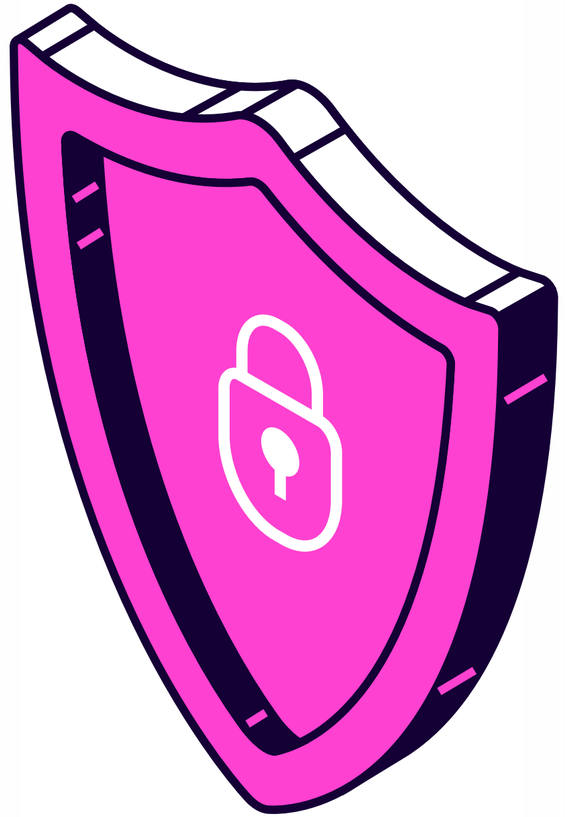
We provides comprehensive techniques for VAPT Services.

- Planning and Scoping
- Information Gathering
- Vulnerability Assessment
- Penetration Testing & Exploitation
- Exploitation & Post Exploitation
- Risk Analysis and Reporting
- Remediation and Re-Testing

ENCODERSPRO

PENTORA FIREWALL

Protect your valuable data with ENCODERSPRO encryption, data loss prevention, and secure firewall solutions.



01.

Risk reduction

Comprehensive Protection For Your Critical Data And Applications.

02.

Firewall Logs

Get attacker’s logs including IP, User Agent, Vulnerable Endpoints, etc.

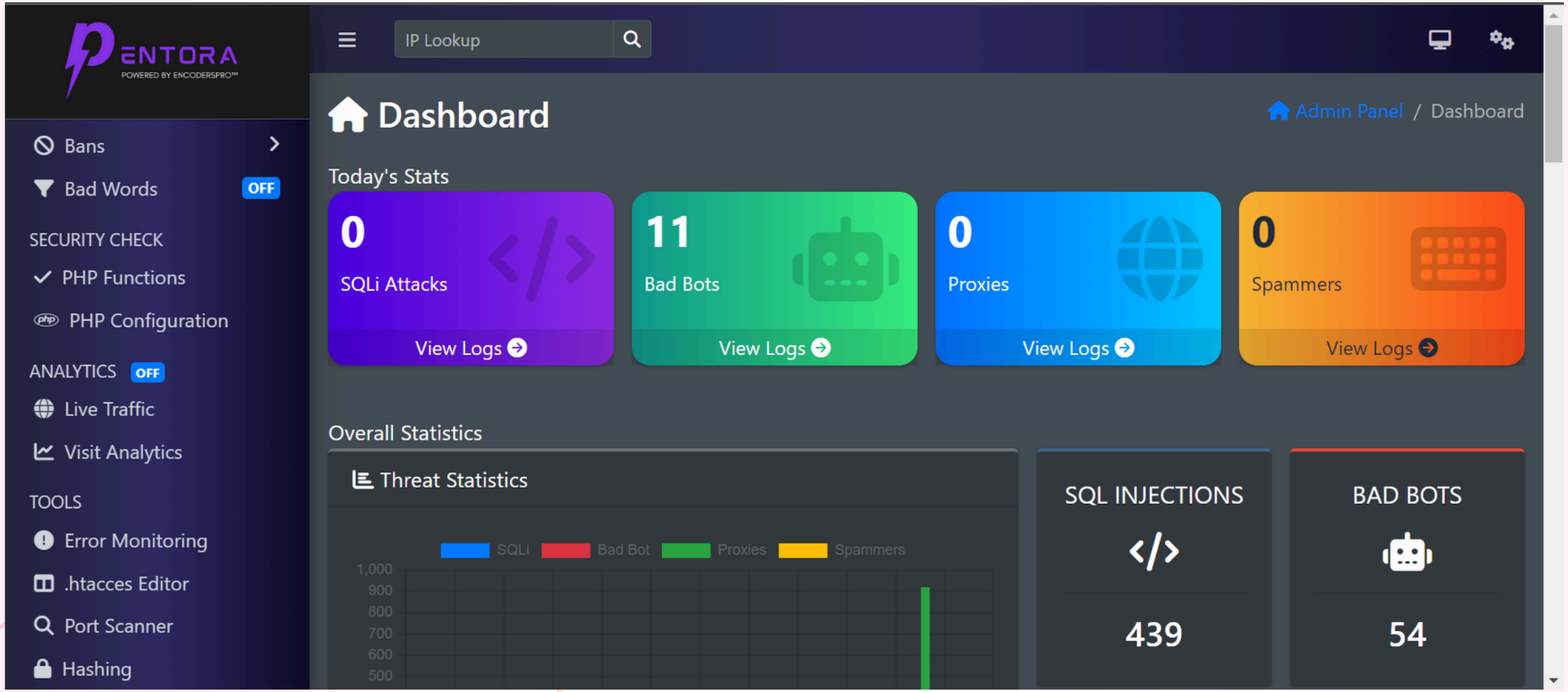
03.

Backdoor Detection

Can detect backdoor and malicious program within the server and source code.

ENCODERSPRO

FIREWALL DASHBOARD



ENCODERSPRO

Wazuh. SOC/XDR

Wazuh is a third party open-source platform that combines Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) capabilities.

01.

File Integrity Monitoring (FIM)

Wazuh's FIM capability allows organizations to track changes to critical files and directories.

02.

Intrusion Detection System (IDS)

Wazuh's IDS capabilities analyze system and application logs.

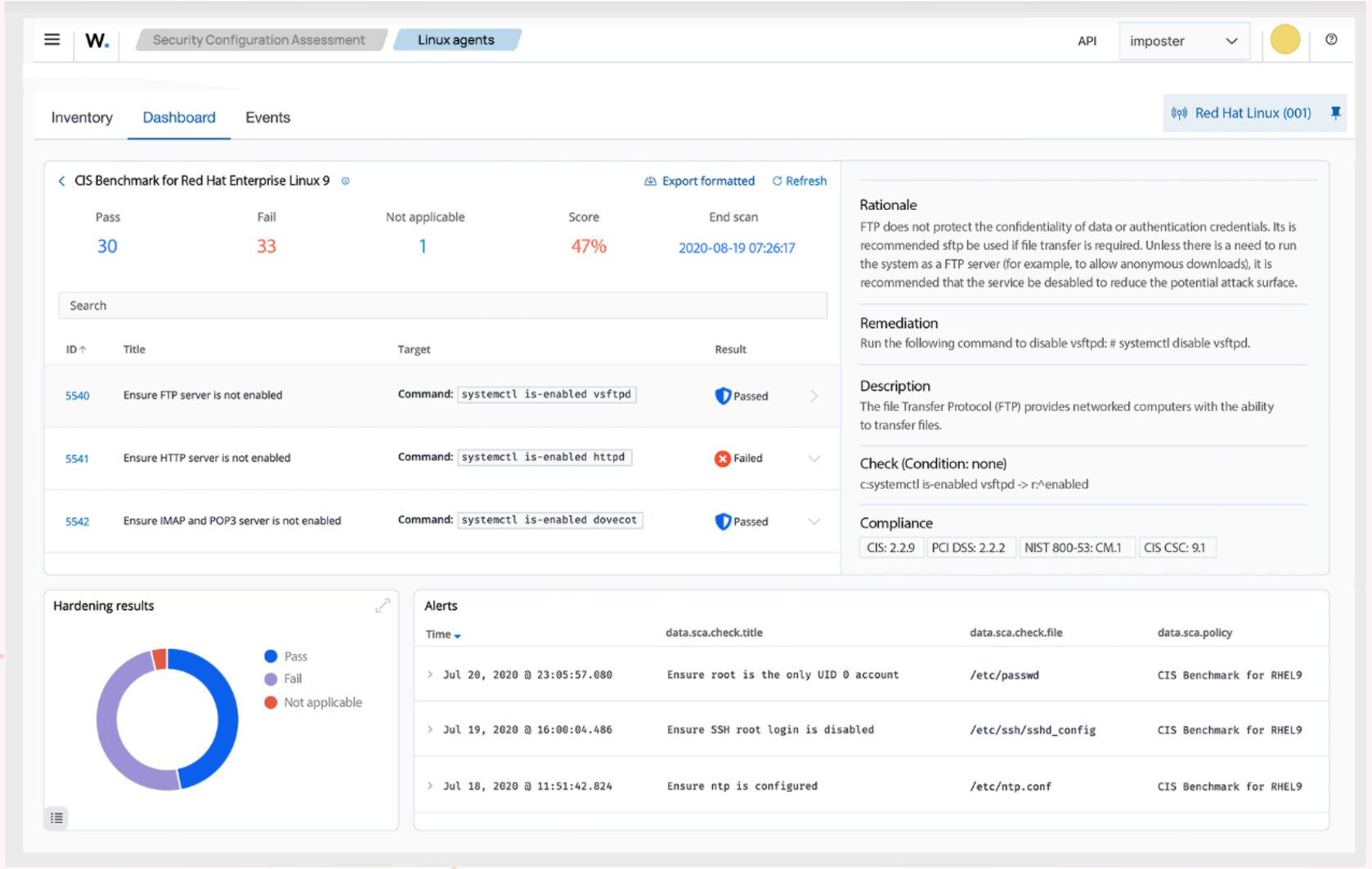
03.

Compliance Management

Provides tools and features to help organizations meet regulatory requirements such as PCI DSS, HIPAA, and GDPR.

ENCODERSPRO

Wazuh Dashboard



ENCODERSPRO

SonarQube Implementation

SonarQube is an open-source platform developed by SonarSource for continuous inspection of code quality to perform automatic reviews with static analysis of code to detect bugs and code smells on 29 programming languages.

01.

Static Code Analysis:

Analyzes code to find vulnerabilities, and code smells without executing it, helping to prevent issues from reaching production.

02.

Vulnerability Detection:

Specifically designed to find deeply hidden security issues in developer-written and AI-generated code.

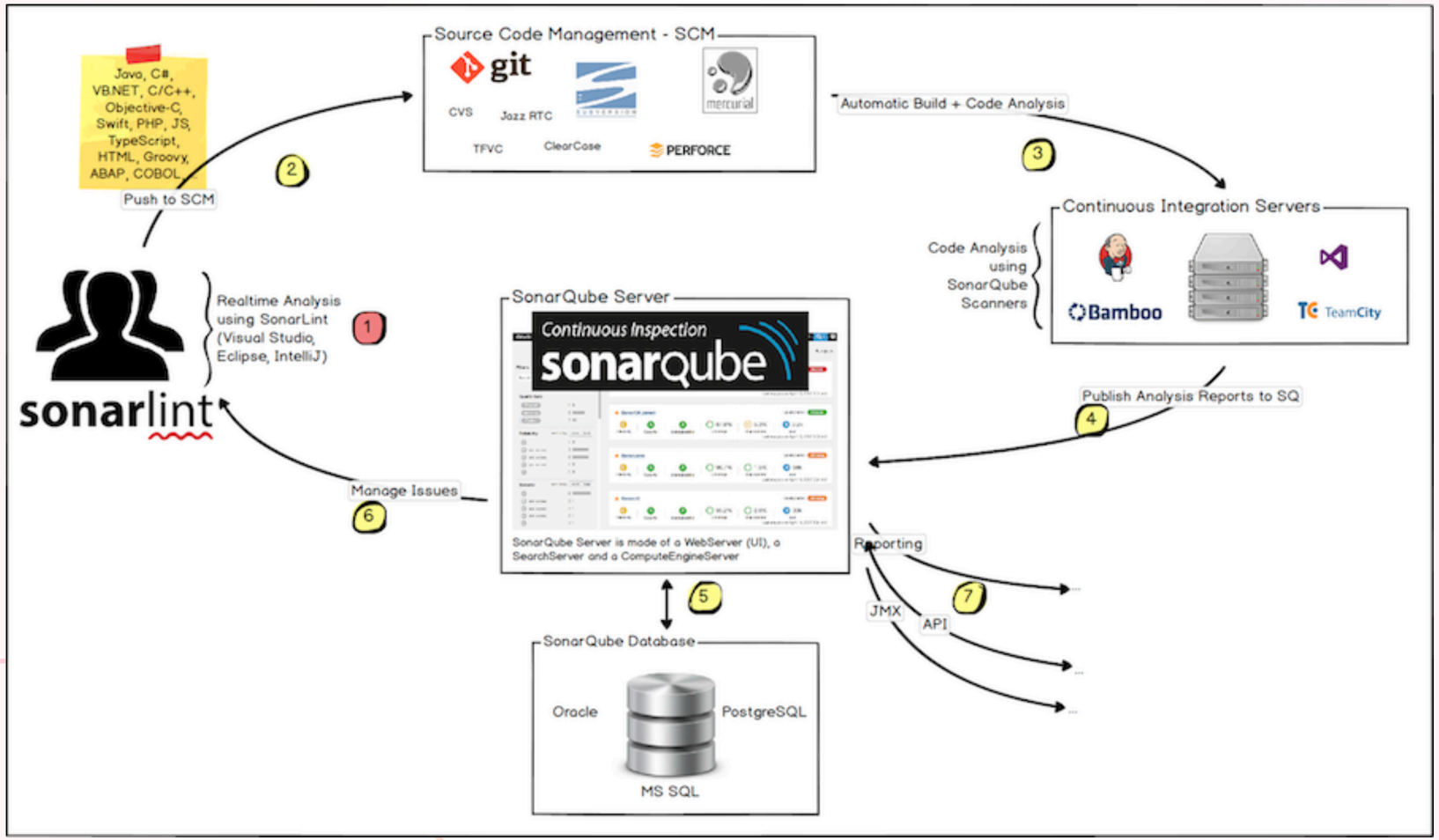
03.

Code Coverage & Test Reports:

Interprets code coverage metrics and provides reports to understand testing effectiveness.

ENCODERSPRO

SonarQube Architecture

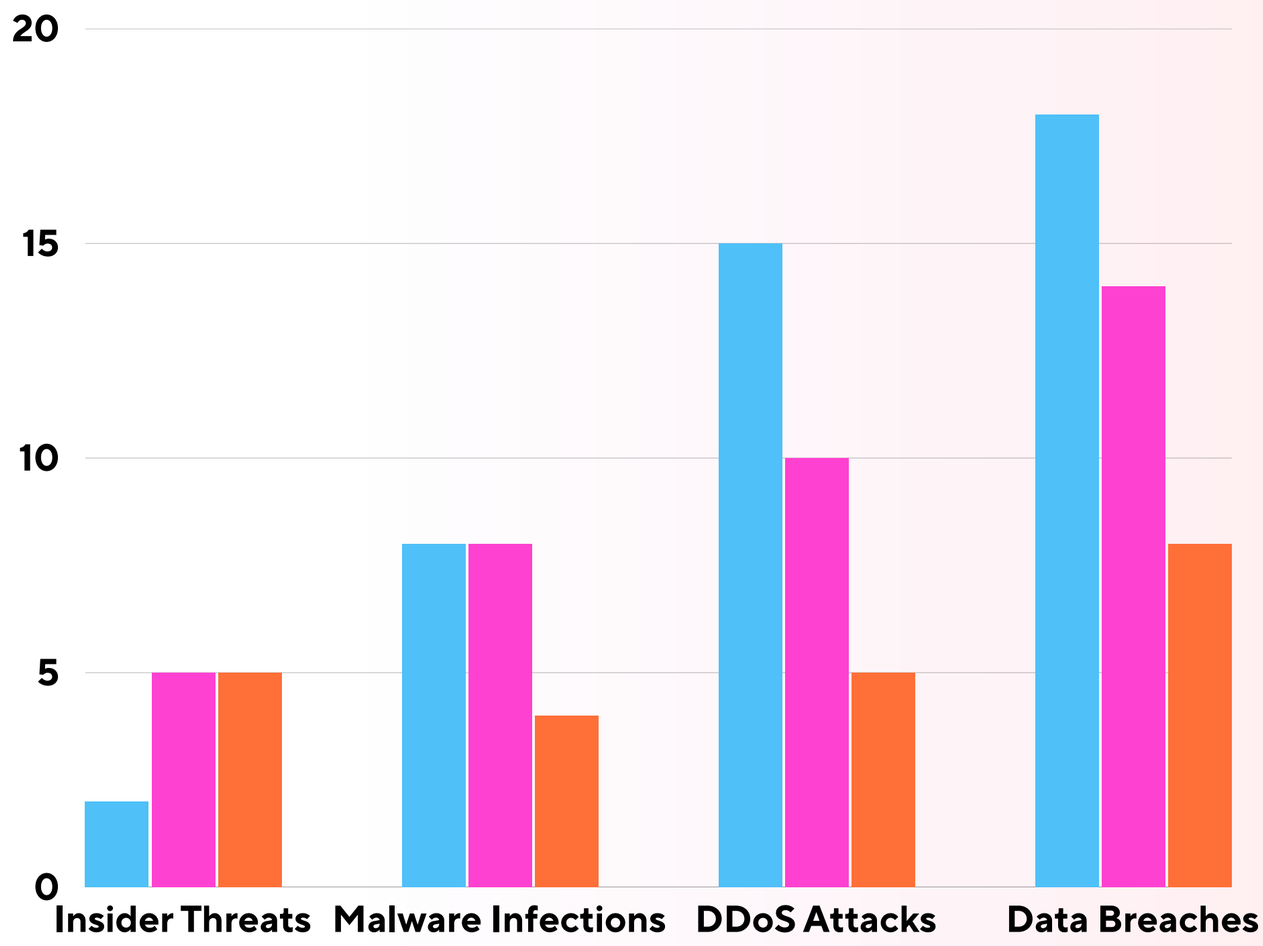


ENCODERSPRO

Get Daily cybersecurity threat report

- Incidents
- Severity (1-10)
- Mitigation

Effective mitigation strategies are in place, with high or medium mitigation levels across incidents.



ENCODERSPRO

Phishing Simulation

A phishing simulation tool, also known as a phishing test, is a program that sends realistic phishing emails to employees to gauge their response to phishing attacks.

01.

Create Campaign

Create your own campaigns for the dedicated employees or staff.

02.

Add Custom Templates

Add your own customized templates for phishing emails.

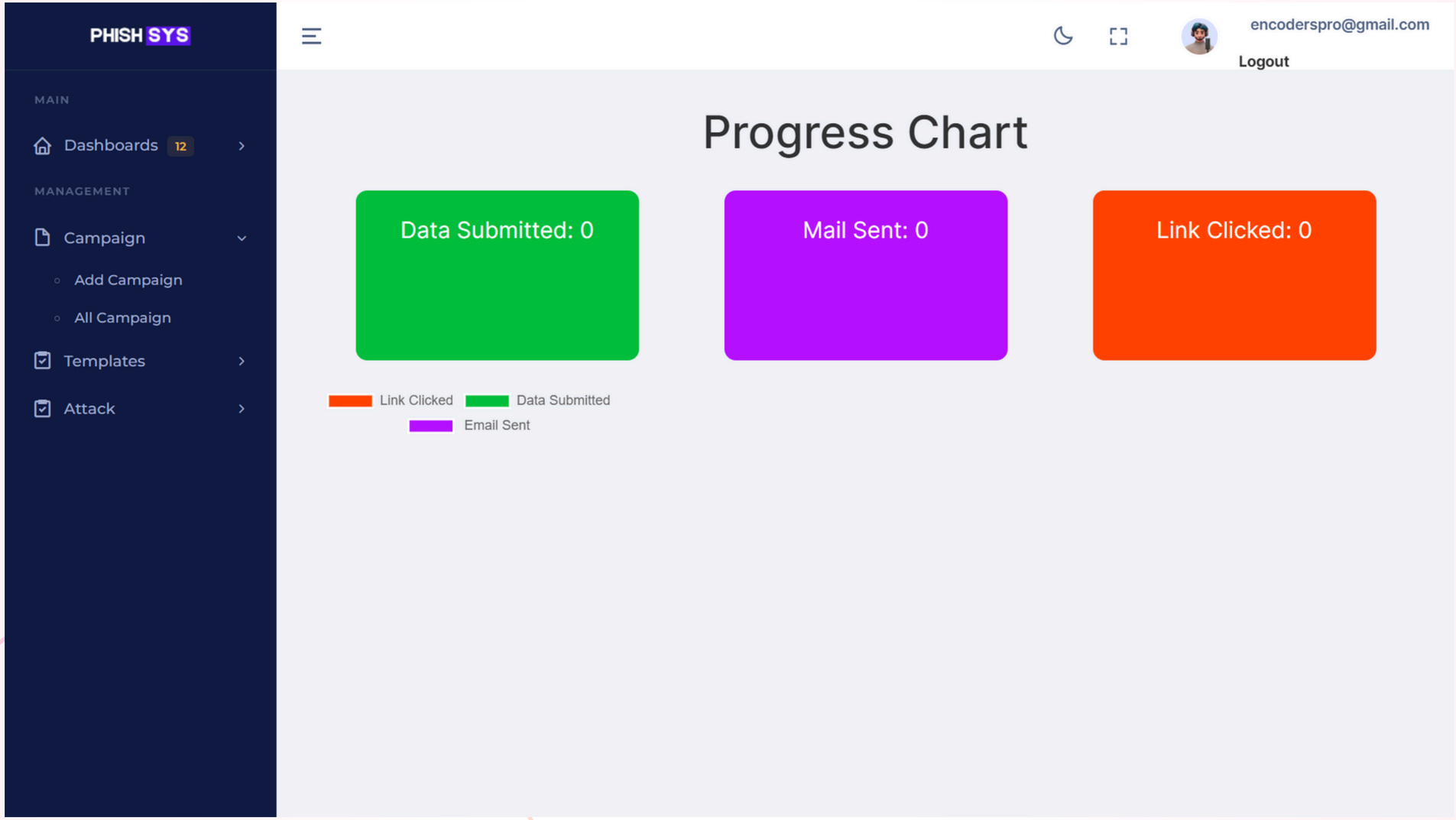
03.

Secure Internal Infra

Secure your internal infrastructure by verifying the internal phishing threats and fix those issues accordingly.

ENCODERSPRO

SIMULATION DASHBOARD



ENCODERSPRO

Our Team Certifications

- OSCP (Offensive Security Certified Professional)
- CPENT (Certified Penetration Testing Professional)
- CEH (Certified Ethical Hacker)
- eJPT (Junior Penetration Tester)
- CCNA, CCNP - Cisco Network Security Certifications
- CNSS (Certified Network Security Specialist)

ENCODERSPRO

Get connect today!

Contact info

+91-9559699100

pentora@encoderspro.com

https://pentora.encoderspro.com

Our office

Kanpur, Uttar Pradesh,
208011