BRUNO DELNOZ

Defensive Cybersecurity Expert • Critical Infrastructure • Blue Team

30+ Years IT • Think Like Attacker to Defend Better

📍 Rochefort, Belgium • 📧 bruno.delnoz@protonmail.com • 📱 +32 456 882 457 💻 github.com/bdelnoz • 💼 linkedin.com/in/delnoz

DEFENSIVE PHILOSOPHY

The best defense comes from understanding the attack. After 30 years in IT and 226+ security projects, I've developed a unique approach: thinking like an attacker to better defend. My offensive WiFi tools (500+ GitHub stars) allow me to understand real attack vectors. My privacy-first expertise (Whisper local STT, zero cloud) demonstrates my confidentiality understanding. A good defender doesn't just deploy firewalls - they anticipate adversary tactics, test their own defenses, and assume breach to prepare detection/response.

ENLIGHTENED DEFENSIVE MINDSET

Think Like Attacker to Defend

- □ **Red team mindset** : My offensive tools (WiFi attacks, pentest) inform my defensive strategies
- □ **Assume breach mentality** : Start from compromise assumption → focus detection/response
- □ **Threat modeling** : Identify probable adversaries, anticipate TTPs, prioritize defenses
- □ **Purple team approach** : Combine offensive + defensive for effectiveness validation
- □ **Continuous improvement** : Incident post-mortems, lessons learned, defense iteration

Defense in Depth

- □ **Layered security** : Perimeter → Network → Host → Application → Data - no single point of failure
- □ **Zero trust architecture** : Never trust always verify, micro-segmentation, least privilege
- □ **Systematic hardening** : Disable unnecessary services, patch management, configuration baselines
- □ **Monitoring & logging** : SIEM, centralized logs, anomaly detection, intelligent alerting
- □ **Incident response** : Prepared playbooks, forensics readiness, crisis communication

Compliance & Governance

- □ **Standards awareness** : ISO 27001, NIST Cybersecurity Framework, CIS Controls
- □ **Risk management** : Risk assessment, prioritization, mitigation strategies, residual risk
- □ **Audit preparation** : Documentation, evidence collection, gap analysis, remediation plans
- □ **Policy development** : Security policies, procedures, guidelines, awareness training

DEFENSIVE TECHNICAL SKILLS

Infrastructure Security (Production Tools)

- □ **iptables firewall** : SystemD auto-boot, strict rules, stateful inspection (GitHub public)
- □ **scan_security** : Security scanning suite (ClamAV, rkhunter, ports, processes) - complete automation
- □ **ssh_control** : SSH hardening, key management, monitoring, fail2ban integration
- □ **usb_enc** : LUKS USB encryption automation, secure key storage
- □ **Network segmentation** : VLANs, ACLs, micro-segmentation, DMZ architecture

Monitoring & Detection

- □ **SIEM basics** : Log aggregation, correlation rules, alerting, dashboards
- □ **IDS/IPS** : Snort/Suricata rules, signature development, false positive tuning
- □ **Network monitoring** : Wireshark deep analysis, NetFlow/sFlow, bandwidth monitoring, anomaly detection
- □ **Threat intelligence** : IOC feeds, MITRE ATT&CK framework, adversary tactics tracking
- □ **Vulnerability management** : Scanning (Nessus, OpenVAS), prioritization, patch orchestration

Encryption & Data Protection

- □ **LUKS mastery** : Full-disk encryption, key management, automated mounting, recovery procedures
- □ **TLS/SSL** : Certificate management, PKI, cipher suite selection, perfect forward secrecy
- □ **VPN** : OpenVPN, WireGuard, IPsec, site-to-site + remote access
- □ **GPG/PGP** : Email encryption, file signing, key management, web of trust
- □ **Backup encryption** : Encrypted backups, secure storage, recovery testing, 3-2-1 rule

System Hardening (30+ years Linux)

- □ **Kali Linux hardening** : Secure daily environment, defensive customization
- □ **CIS benchmarks** : Automated hardening scripts, compliance validation, remediation
- □ **SELinux/AppArmor** : Mandatory access control, policy development, troubleshooting
- □ **Kernel hardening** : sysctl tuning, module blacklisting, security features activation
- □ **Service minimization** : Disable unnecessary services, port reduction, attack surface minimization

Identity & Access Management

- □ **Authentication** : OAuth 2.0, SAML 2.0, OpenID Connect, JWT - Axway middleware expertise
- □ **MFA/2FA** : TOTP, hardware tokens, biometrics, passwordless authentication
- □ **Privilege management** : sudo hardening, PAM configuration, least privilege, separation of duties
- □ **PKI** : Certificate lifecycle, CA hierarchy, revocation, HSM integration
- □ **SSH keys** : Key rotation, authorized_keys management, certificate-based auth

PROJECTS DEMONSTRATING DEFENSIVE APPROACH

Security Automation

- □ **iptables firewall** : Auto-deploy SystemD, strict rules, logging - github.com/bdelnoz
- □ **scan_security** : Automated scanning suite (malware, rootkits, ports, processes)
- □ **ssh_control** : SSH monitoring + hardening automation
- □ **backup automation** : Encrypted backups, rotation, verification, alerting

Privacy & Confidentiality (Data Defense)

- □ **braveVTTextension v3.0** : Whisper local STT (zero cloud) - privacy-first defensive approach demonstration
- □ **usb_enc** : LUKS USB encryption automation - data at rest protection
- □ **regles_contextualisation** : V110 - demonstrates sensitive information protection understanding

Offensive Tools = Defense Validation

- □ **cmd.airmon-dos** : WiFi DoS testing - used to test my own network robustness
- □ **scripts-wifi-scan** : WiFi reconnaissance - audit my own wireless exposures
- □ **pentestAPK** : Mobile app testing - validate application security before deployment
- □ **NoXoZVorteX** : Data analysis - understand adversary patterns in communications

PROFESSIONAL EXPERIENCE

Axway Software - Senior Consultant (2007-2018, 11 years)

- □ **40+ critical middleware projects** : 98% success rate, high-availability infrastructure
- □ **Critical flow security** : OAuth/SAML/JWT, transit encryption, API security, compliance
- □ **French Government** : Ministry of Finance (Macron administration) - sensitive infrastructure
- □ **Certified trainer** : Security best practices transmission, threat modeling, defensive architecture
- □ **Multi-country** : France, Belgium, Luxembourg, international - multi-jurisdiction compliance

Freelance Consultant AI/ML & Security (2024-2025)

- □ **11 production applications** : Privacy-first tools, AI workflow security
- □ **500+ GitHub stars** : Community recognition for security code quality
- □ **Security research** : AI security, prompt injection defense, LLM safety
- □ **Open source** : Defensive tools contribution, protection knowledge sharing

COMPLEMENTARY TECHNICAL SKILLS

Scripting & Automation

- □ **Bash expert** : 109+ production scripts, 25+ years, complete defense automation
- □ **Python 3** : 37+ projects, security tooling, SIEM integration, log parsing
- □ **Infrastructure as Code** : Ansible basics, configuration management, reproducible hardening

Cloud & Containers

- □ **Docker security** : Image hardening, scanning, runtime security, least privilege
- □ **CI/CD security** : GitHub Actions, secret management, SAST/DAST integration
- □ **Cloud basics** : AWS/Azure security groups, IAM, encryption at rest/transit

Network & Infrastructure

- □ **Network architecture** : Deep TCP/IP, routing, VLANs, VPN, micro-segmentation
- □ **Firewall management** : iptables/nftables, stateful inspection, geo-blocking, rate limiting
- □ **DNS security** : DNSSEC, DoH/DoT, RPZ, filtering, monitoring
- □ **Load balancing** : HAProxy, nginx, TLS termination, health checks, failover

CERTIFICATIONS & CONTINUOUS TRAINING

- □ **CCSP (in progress)** : 6 courses completed - Cloud security, cryptography, compliance
- □ **Autodidact** : 30 years autonomous learning, daily security watch
- □ **Standards awareness** : ISO 27001, NIST CSF, CIS Controls, GDPR compliance
- □ **Certified Axway trainer** : Defense knowledge transmission, secure architecture

VALUE PROPOSITION

Enlightened Defensive Approach

- □ **Think like attacker** : My offensive tools inform my defensive strategies - not theoretical
- □ **Natural purple team** : Combines red + blue team perspectives for effectiveness validation
- □ **Production proven** : GitHub portfolio demonstrates daily-used tools, not just slides

Critical Infrastructure

- □ **High availability** : Axway 40+ critical projects, French Government (Ministry of Finance)
- □ **Multi-jurisdiction compliance** : France, Belgium, Luxembourg - different standards mastered
- □ **Encryption mastery** : LUKS, TLS/SSL, VPN, GPG - data at rest + transit protection
- □ **Monitoring automation** : Production scripts for anomaly detection, intelligent alerting

Knowledge Transfer

- □ **Certified trainer** : Axway - best practices transmission, threat modeling, architecture
- □ **Comprehensive documentation** : All GitHub projects documented - README, INSTALL, USAGE, CHANGELOG
- □ **Mentorship** : 30+ developers mentored, 200+ training hours, knowledge multiplier
- □ **Open source contribution** : Defensive tools sharing, 500+ stars community

ADDITIONAL INFORMATION

- □ **Location** : Rochefort, Belgium - Immediate availability
- □ **Languages** : French (native), English (professional - technical reading/writing C1)
- □ **GitHub** : github.com/bdelnoz - Public defensive tools portfolio
- □ **Web portfolio** : bdelnoz.github.io - Detailed technical CV
- □ **Security clearance** : Available upon request

30 Years IT • Critical Infrastructure • Think Like Attacker to Defend Better • 500+ GitHub Stars
📍 Rochefort, Belgium • 📧 bruno.delnoz@protonmail.com • 📱 +32 456 882 457 💻 github.com/bdelnoz • 💼 linkedin.com/in/delnoz