DEFENSIVE SECURITY

In & Out EXFIL Platform.
Draft.

PLATFORM OVERVIEW:

In & Out EXFIL Platform by Defensive Security is a distributed, post-exploitation and lateral movement simulation platform that allows for safe and automated validation of your existing IT security solutions against modern network malicious techniques and adversaries behavior.

In terms of data leakage protection and for better understanding a current status of your network security posture, the In & Out EXFIL Platform helps you identify risks, network security blind spots and unexpected, uncovered spaces by simulating a real, offensive, cyber adversary network behavior just from Web UI.

HOW IT WORKS:

- The core of In & Out EXFIL Platform is an engine powered by a combination of advanced exfiltration techniques with tunneling and pivoting jobs. It can be run in single or multi node architecture using wide range of protocols and services, APT-style modules and C2 tricks.

- A built-in EXFIL Jobs Definition Library allows for choosing and running sophisticated network behaviors easily by using friendly, dedicated web UI.

- You can choose between simulation of single job on demand or you can schedule chained EXFIL Job events for running advanced "EXFIL campaigns" in continuous manner.

- It generates a real traffic of all phases of sophisticated attacks, including internal reconnaissance, malware C2 connections, data exfiltration, tunneling and pivoting between critical network segments or egress and many other hidden types of malicious communications.

- Virtual console for a real-time tracing (full output) of running exfiltration jobs.

- Simulated C2 infrastructure hosted in the cloud eliminates the need to install and maintain hundreds of tools, dependencies, IPs, domains and argument operations.

- Reporting module delivers you a complete job results with low-level details by default.

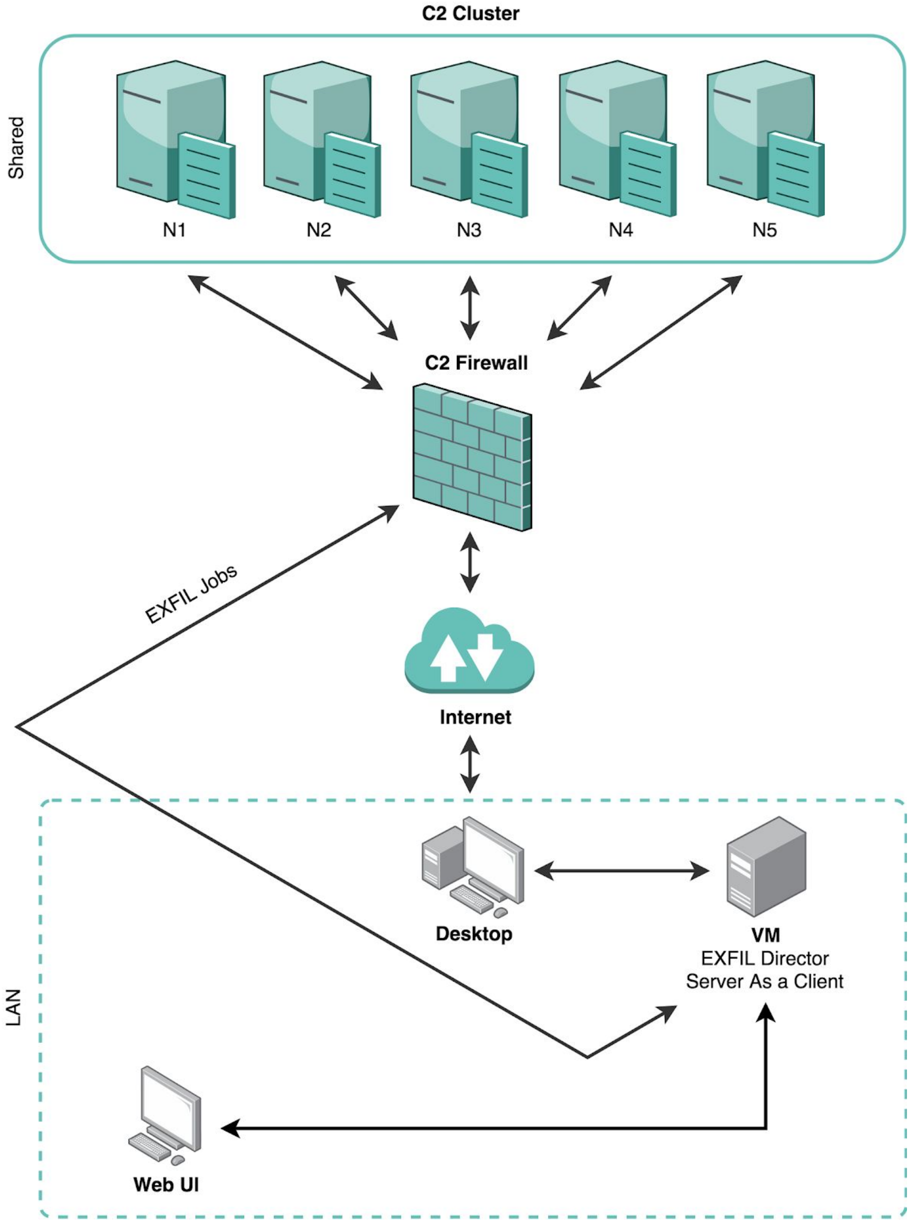
- Become confident that your network security really works!

ARCHITECTURE → CORE COMPONENTS:

- EXFIL Director VM
- EXFIL Jobs Library
- EXFIL Node VMs
- Smart Proxy VM
- Web UI
- C2 Cloud Infrastructure

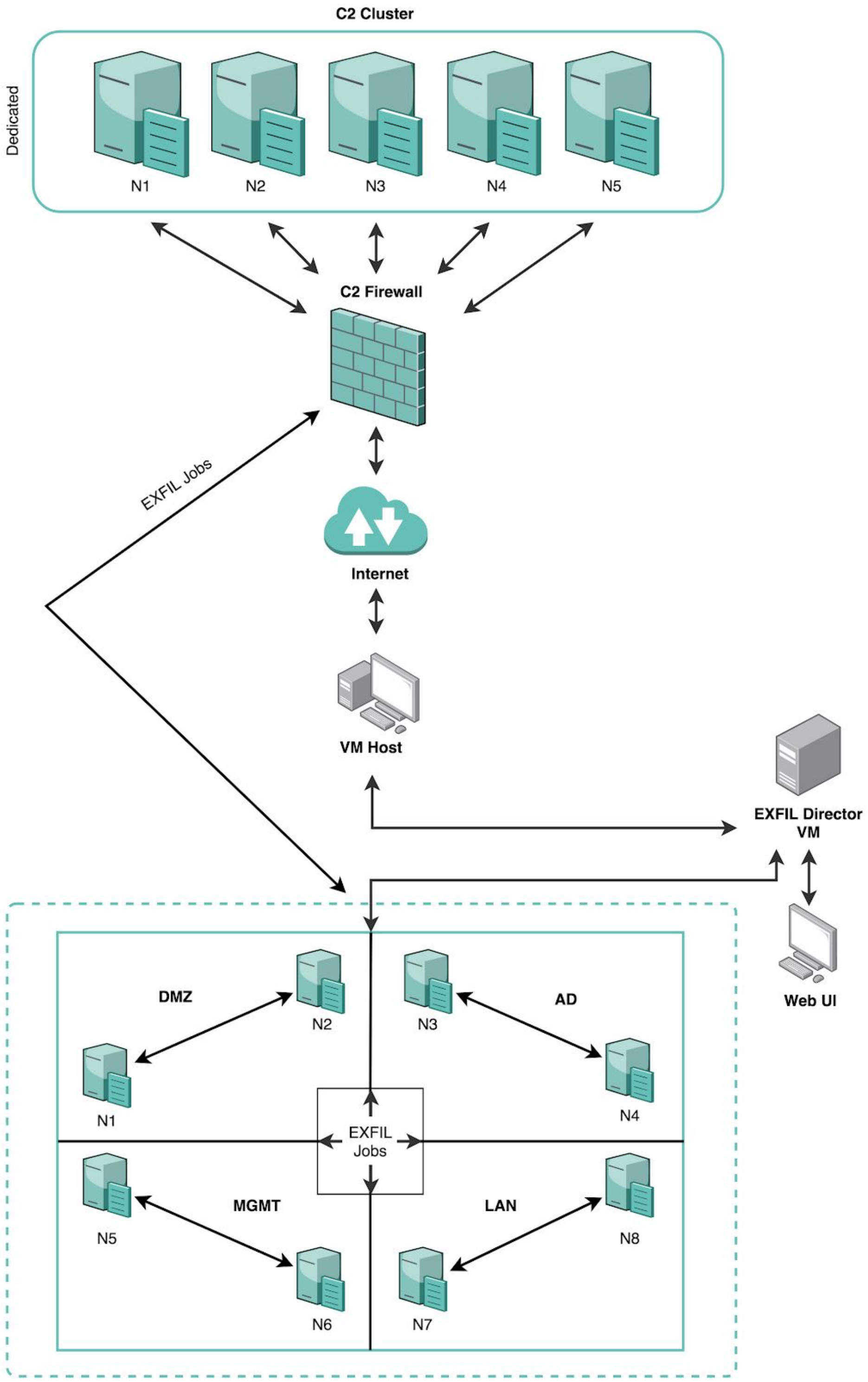
ARCHITECTURE → SINGLE NODE (Individual / SaaS for Business):

- Server as Client
- EXFIL Jobs Library as a functionality core
- Single Traffic direction only (int2ext)
- Shared / dedicated C2 Cloud Infrastructure



ARCHITECTURE → MULTI NODE (Enterprise):

- EXFIL Director VM as a head of job execution
- SSH based job execution / Smart Proxy
- Multi-direction traffic (int2ext, int2dmz, dmz2ad, ad2mgmt, ad2ad, int2int, etc.)
- Dedicated C2 Cloud Infrastructure



ARCHITECTURE → C2 CLOUD INFRASTRUCTURE:

- C2 Firewall / balancer
- External DNS
- Integrated part of a service
- VPS-based

REPORTING:

- EXFIL Jobs / state History
- E-mail notification
- Dedicated API / logs → SIEM integration

KNOWLEDGE BASE:

- In-use jobs and open source tools descriptions and howtos
- TTP from MITRE ATT&CK Framework
- Emerging threats & TTP update

BUSINESS VALUE PROPOSITIONS:

- Easy measurement and verification if your current network security solutions meet the compliance policy assumptions

- Fast validation if your IDS, IPS, DLP, NG-Firewall, Enterprise Proxy, Risk Scoring and hybrid Machine Learning solutions work as expected

- Better handling and understanding of a correlation between generated security events, network traffic and log entries with focus on finding potential protection failures of controls

- Planning infrastructure security improvements and choosing the best IT Security solutions in the market

- Support in creating complex TTP scenarios based on MITRE ATT&CK Framework

- Knowledge transfer - continuous learning about details of sophisticated network data exfiltration tricks and post lateral movement actions you have not been aware before

- Demonstrating the value on SOC/SIEM/IT Security investments to the Executive Board using the real world “offensive vs defensive” use-cases by using “click, play & report ” approach

- Openness for feature requests

- Dedicated technical training sessions

BUSINESS VALUE NEEDS:

- Help in building a stable, substantive brand in a global IT Security market
- Validation of development direction and presentation of expectations regarding functionality in relation to current and future needs
- Professional fees
- Mentoring support of market leader and sharing opinions
- Openness for Proof of Value / Proof of Concept program

KNOWLEDGE TRANSFER:

- EXFIL Job descriptions
- MITRE Mapping services
- Training / workshops
- Reports
- Threat newsletter

DEFENSIVE SECURITY CORE TEAM:

- Leszek Miś:
    - Founder at Defensive Security, Principal Trainer and Security Researcher with over 15 years of experience in Cyber Security and Open Source Security Solutions market. He went through the full path of the infosec carrier positions: from OSS researcher, Linux administrator and system developer, Solution Engineer, DevOps/CI, through penetration tester and security consultant delivering hardening services and training for the biggest players in the European market, to become finally an IT Security Architect / SOC Security Analyst with

deep non-vendor focus on Network Security attack and detection. He’s got deep knowledge about finding blind spots and security gaps in corporate environments. Perfectly understands technology and business values from delivering structured, automated adversary simulation platform.

- Recognized speaker and trainer: BruCON, Black Hat USA, OWASP Appsec USA, FloCon USA, LayerOne LA, 44CON UK, Hack In The Box DBX/AMS/SG, Infosec in the City SG, Nanosec Asia KL, Confidence PL, PLNOG, Open Source Day PL, Red Hat Roadshow. Member of OWASP Poland Chapter.

- Holds many certifications:
  - OSCP
  - RHCA
  - RHCSS
  - Splunk Certified Architect

- Krzysztof Koszyka:
  - A highly experienced Software Engineer with over 15 years’ practice. Participation as a developer and technical leader in many projects related with backend and server services. He led and deployed projects for high scalability servers in one of the biggest data centers in Poland (Onet.pl). Experience with embedded systems around low level and security layers (Intel Corp.). Strong and technical researcher (patent co-inventor) especially for topics related with network protocols and security aspects. Technology enthusiast and flexible developer with skills in most current development languages.

  - He graduated from the Technical University of Cracow with two master’s degrees in technical physics and computer science. Experienced also in startup projects as a technical leader and business strategy player.

- Magdalena Miś:
  - Magdalena Miś founded Emerge in 2007 and throughout all years has helped in all financial and business aspects of its development.
She spent most of her career in positions related to accounting and controlling. She has worked in well-known and recognized outsourcing companies in the field of accounting and large entities in the commercial and production sectors, where she was also involved in due diligence, M&A and audit projects. Her scope includes ongoing financial settlements, taxes, accounting, budgeting, issuing opinions and negotiating contracts and optimizing the legal structures of new ventures.

        - Holds a master's degree in finance in the field of accounting, but she is an advocate of investing in new, revolutionary technologies of the future.

    - Maciej Drobniuch:
        - Focused on all security aspects on each possible layer, passionate and devoted towards making everything flawless and user friendly while delivering real value without making compromises. Past member of a global Professional Services Team @Akamai focused on DDoS attack mitigation where he was working as a Security Solutions Architect for major brands around the world. DevOps, Security researcher and malware reverse engineer at Collective Sense where he worked on training Machine Learning models against malicious traffic on the system and network layer. Extremely passionate about cloud automation solutions and cloud architecture.

        - Sensitive about business and technology ecosystem. Fascinated about process optimization and business management. Real team player and motivated achiever. Hungry for knowledge and the unknown.

CURRENT CUSTOMERS AND RECOMMENDATIONS:

- PZU
- ING Tech
- PGNiG
- Integrated Solutions
- Warta
- AXA
- Aviva
- Stack Overflow
- Daily Motion
- Alior Bank
- Ministry of Finance
- Millennium Bank
- Netart
- Rekord Systemy Informatyczne
- IBS
- Cinkciarz
- Rockwell Automation
- Esky

- LPP
- ARiMR
- TUV
- Polkomtel
- Infovide Matrix

---

*SESSIONS @ CONFERENCES:

- BruCON BE→ Ghent
- Hack In The Box → Dubai / Amsterdam / Singapore
- Infosec in The Box → Singapore
- OWASP AppSec USA → Orlando
- 44CON UK → London
- Black Hat USA → Las Vegas
- X33FCON PL → Gdynia
- Confidence PL → Cracow
- PLNOG → Warsaw
- Open Source Day PL → Warsaw
- CCCE → Copenhagen
- Nanosec Asia → Kuala Lumpur
- Gigacon PL
- OWASP Poland Chapter
- Red Hat Roadshow

CONTACT:

- Email: leszek.mis@defensive-security.com / info@defensive-security.com
- Mobile: +48 791 611 309
- Website: https://www.defensive-security.com