DEFENSIVE SECURITY

PurpleLabs, Training Portfolio & Services.

Cyber Security Skills Development
& Knowledge Transfer.

About Us

DEFENSIVE SECURITY

15+

years of experience
in **Cyber security** market

1000+

trained **students**
globally

- **Dedicated hands-on training programs for Red, Blue and Purple teams**

RED TEAM · PURPLE TEAM · BLUE TEAM

- **Cyber security Educational Services**

BRUCON · black hat USA · 44CON London · AppSec USA

AMSTERDAM
SINGAPORE
DUBAI

HITB+CyberWeek
Abu Dhabi, UAE

- **Professional Services**


Adversary Simulations


Threat Hunting


Penetration Testing


Security Analytics


Network Security & Hardening

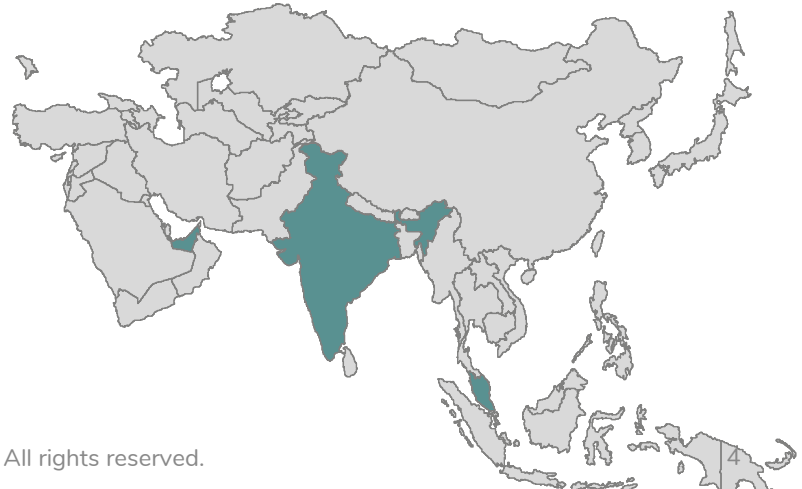

Open Source Security for SOC

Copyright © Defensive Security All rights reserved.

US
Brazil
Sweden
Netherlands
UK
Belgium
Poland
Germany
France
Italy

Global scope

Austria
Czech
UAE
India
Malaysia
Singapore



Copyright © Defensive Security All rights reserved.

MEET OUT **TRAINER**

LESZEK MIŚ

2017/18	BruCON
2018	OWASP Appsec US | FloCon USA
2018/19	Hack In The Box Dubai/Amsterdam/Singapore/Abu Dhabi
2019	44CON UK | Black Hat USA
2019	Confidence PL | PLNOG | Open Source Day PL | Secure PL | Advanced Threat Summit PL

Leszek Miś is the Founder of 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 DevOps, 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 2017/2018, Black Hat USA 2019, OWASP Appsec US 2018, FloCon USA 2018, Hack In The Box Dubai / Amsterdam / Singapore / Abu Dhabi 2018/2019, 44CON UK 2019, Confidence PL, PLNOG, Open Source Day PL, Secure PL, Advanced Threat Summit PL 2019.

Holds many certifications: OSCP, RHCA, RHCSS, Splunk Certified Architect.

His areas of interest include network "features" extraction, OS internals and forensics. Constantly tries to figure out what the AI/ML Network Security vendors try to sell. In free time he likes to break into "IoT world" just for fun.

Still learning hard every single day

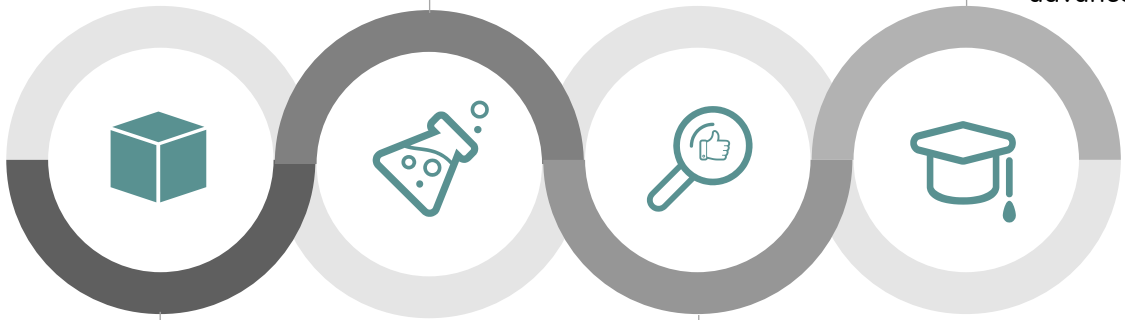
Copyright © Defensive Security All rights reserved.

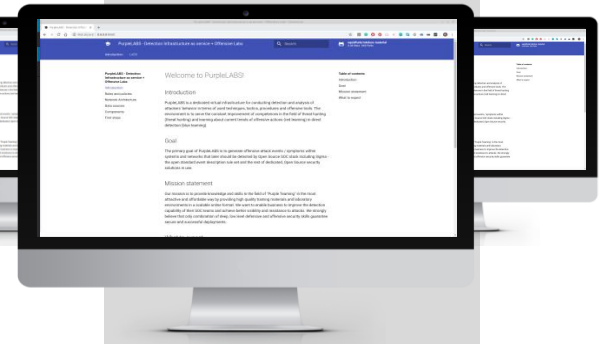
PurpleLABS
all in one

DEFENSIVE SECURITY

2 Adversary laboratory
breach-and-simulation exercises

4 Dedicated Cyber Trainer
dedicated Trainer with support and advanced lessons





1 Infrastructure Ready-to-go
Network/system visibility in central places

3 Detection through attack
Flip Mode style driven by Sigma rules

Copyright © Defensive Security All rights reserved.

PurpleLabs.

Virtual Detection Infrastructure as Service + Offensive LABS.

PurpleLabs

DEFENSIVE SECURITY

Dedicated virtual infrastructure for conducting detection and analysis of adversary behaviors

Analytical interfaces for all important data sources

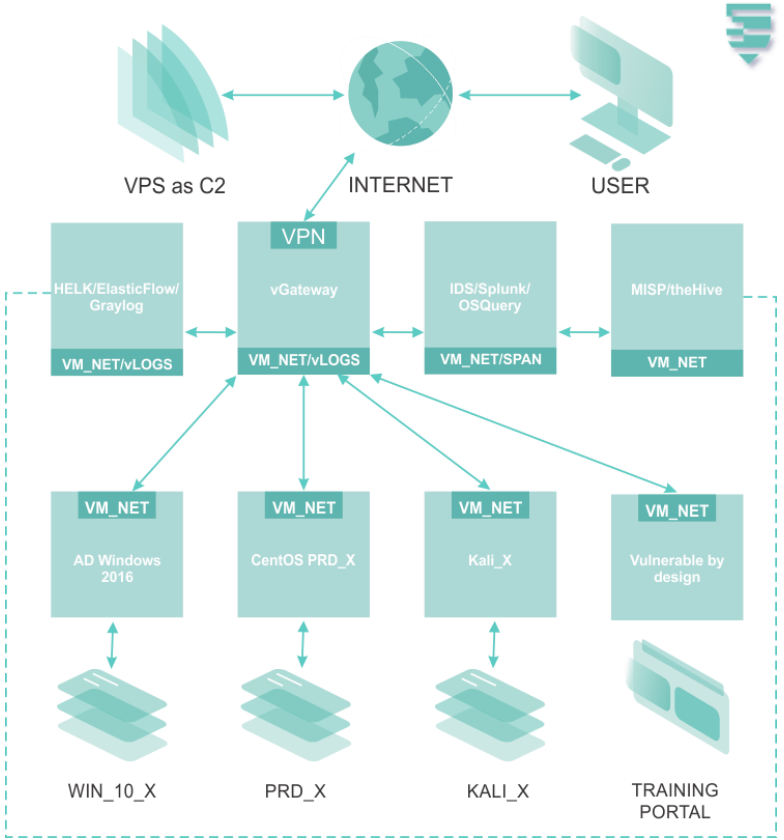
Sysmon & Windows events | Firewall logs | Netflow | Zeek | Suricata

oSquery | System/ authent. logs | PowerShell logs | WAF logs | Proxy logs | Audit logs

Allows for learning about current trends of offensive actions (red teaming) vs detection points (blue teaming)

Hunting friendly

Focuses on Open Source Security Software



Copyright © Defensive Security All rights reserved.

PurpleLabs
Infrastructure

DEFENSIVE SECURITY

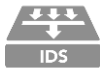
AD Windows
Domain Controller 2016

Windows 10
workstations

CentOS
Ubuntu Linux servers

Kali Linux
desktops

vSPAN
vNetflow



IDS/HIDS

Log aggregators
And collectors

Security event
analytics solutions

WAF / Proxy server

SSH Jump host

Vulnerable
by design host

Incident Response
Platforms

Virtual Private Servers
as external C2 Instances

Copyright © Defensive Security All rights reserved.

PurpleLabs Goals

Attack events

Generate offensive attack events / symptoms and detect them by using Open Source SOC stack based on Sigma rules:

- Generic Signature Format for SIEM Systems
- Open standard security event description rule-set

Improve detection

Improve detection capability of your SOC teams and achieve better visibility and resistance to attacks

Flip mode

learn detection through attack in an attractive, standardized format driven by the Open Source community

Detection as Code vs Adversary Simulations

Use “Detection as Code vs Adversary Simulations” unique approach and increase your level of knowledge in RED / BLUE / PURPLE scope

Brake routine

Detection does not have to be boring and tedious!

Copyright © Defensive Security All rights reserved.

PurpleLabs
Added Values

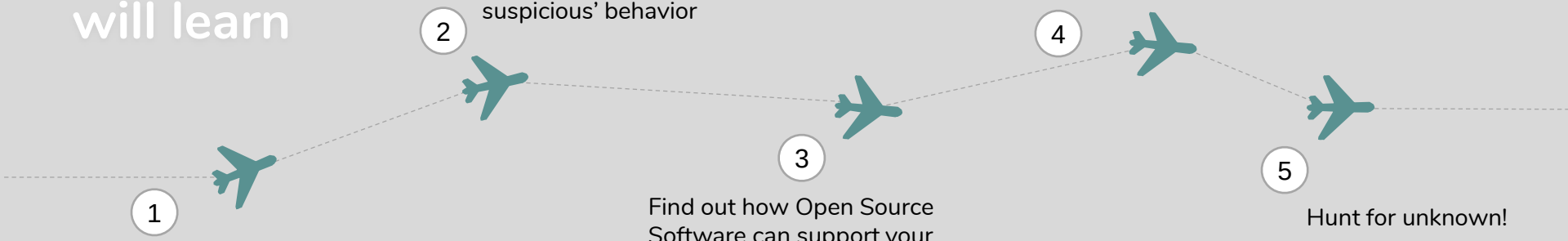
1 **Offensive LABS**

a set of dedicated offensive/defensive hands-on lab instructions

2 **Full content transparency**

list of available labs + short description shared publicly

What you will learn



1 Prepare your SOC team for fast filtering out network noise and allow for better incident response handling

2 Profile your critical OS and network segments in terms of ‘normal vs suspicious’ behavior

3 Find out how Open Source Software can support your SOC infrastructure from red and blue perspective

4 Learn current trends, techniques, and tools for network exfiltration, lateral movement and post-exploitation attack phases

5 Hunt for unknown!

PRICING PLAN

Bussines plan

- 30/60/90 days PurpleLabs access
- Offensive LABS:
  - 5 users
  - 10 users
  - 20+ users

Starting from
1 999 EUR
monthly

Individual plan

- 30/60/90 days PurpleLabs access

Starting from
499 EUR
monthly

DEFENSIVE SECURITY

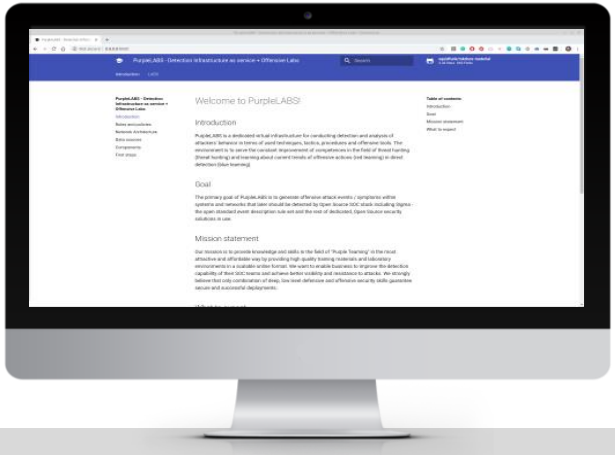
Request
Demo
access

Try for free

Ask for details
purplelabs@defensive-security.com

Copyright © Defensive Security All rights reserved.

DEFENSIVE SECURITY



SUBSCRIPTION PACKAGE **INCLUDES**

VPN access to PurpleLABS cloud Infrastructure

Online Purple training materials

Dedicated Windows 10, CentOS and Kali Linux per student

Pre-configured remote VPS per student

1. **New lab instructions every single month including attack and detection phases**
2. An arsenal of configured simulation tools and C2 frameworks available by default
3. Mapping APT techniques to chained scenarios, Sigma rules and MITRE ATT&CK Framework detection
4. 1 hour of video conference Q&A slot per week
5. Access to Slack channel and private online support service

Copyright © Defensive Security All rights reserved.

DEFENSIVE SECURITY

Training portfolio.

Cutting edge cyber security educational services.

DEFENSIVE SECURITY

SELinux
Development & Administration of Mandatory Access Control Policy

In & Out
Network Exfiltration and Post-Exploitation Techniques
RED Edition

In & Out
Detection of Network Exfiltration and Post-Exploitation Techniques
BLUE Edition

Open Source Defensive Security
The Trinity of Tactics

In the Cloud
Docker Security

In the Cloud
Kubernetes Security

Training portfolio

Copyright © Defensive Security All rights reserved.

In & Out
RED EDITION

RED TEAM

The In & Out - Network Exfiltration and Post-Exploitation Techniques [RED Edition] training class has been designed to present students modern and emerging TTPs available for network exfiltration and lateral movement phases. This highly technical content and only a hands-on practical approach guarantee that the usage of this transferred knowledge & technologies in real production environments will be easy, smooth and repeatable.

Using an available set of tools, the student will play one by one with well-prepared exfiltration, pivoting and tunneling use-cases to generate the true network symptoms of a modern attacker's behavior. Great content for SIEM / SOC team validation including verification methods and techniques for product and service providers from IT Security space → in terms of internal testing and PoC / PoV programs.

Time Duration

3 days (9:00am - 5:00pm)

Who should attend

- Red and Blue team members
- Security / Data Analytics
- CIRT / Incident Response Specialists
- Network Security Engineers
- SOC members and SIEM Engineers
- AI / Machine Learning Developers
- Chief Security Officers and IT Security Directors

More information

https://www.defensive-security.com/training-workshops/in-out-network-exfiltration-and-post-exploitation-techniques-red

DEFENSIVE SECURITY

Agenda

- Introduction to Adversary Simulations and Open Source Attack Emulation projects.
- Modern RAT's implementation and popular APT/C2 malware communication design - the review of the latest APT campaigns mapped to MITRE ATT&CK Framework.
- Not just the basics of TCP/UDP bind and reverse shells.
- Covert channels and C2 techniques.
- Lateral movement and Offensive Frameworks.
- Cloud-based exfiltration techniques and C2 channels.
- FW / WAF protection for your C2 infrastructure.
- Signature-based event analytics, rule bypassing & malicious network traffic generation.
- Summary → recommended defensive/protection tactics, tools, and commercial platforms.

Copyright © Defensive Security All rights reserved.

In & Out
BLUE EDITION

An advanced lab-based training created to present participants:

- Significance of security events correlation including context to reduce the number of false positives and better detection of adversary activities
- Advanced detection methods and techniques against exfiltration and lateral movement including event mapping, grouping, and tagging
- Understand the tactics and behaviors of the adversary after gaining initial access to the network (Linux/Windows)
- Detection methods of tunneling, hiding, pivoting and custom, simulated malicious network events
- Capabilities of many popular Open Source tools and integration with 3rd party security (IDS/IPS/WAF/EDR) and analytics solutions against adversaries' actions
- Verification methods and techniques for product and service providers from IT Security space → in terms of internal testing and PoC / PoV programs

Time Duration

3 days (9:00am - 5:00pm)

Who should attend

- Red and Blue team members
- Security / Data Analytics
- CIRT / Incident Response Specialists
- Network Security Engineers
- SOC members and SIEM Engineers
- AI / Machine Learning Developers
- Chief Security Officers and IT Security Directors

More information

https://www.defensive-security.com/training-workshops/in-out-network-exfiltration-and-post-exploitation-techniques-blue

DEFENSIVE SECURITY

Agenda

- The value behind Adversary Simulations.
  MITRE Attack Framework for APT detection.
- Open Source Security Software for your Security Operation Center - introduction to cloud-based LAB environment and more.
- Network baseline profiling and hunting for malicious events - BRO / Suricata IDS.
- Low-level analysis of Sigma rules + Sysmon for better lateral movement detection.
- Auditing subsystems: auditd, eBPF, OSquery.
- Web security - using WAF for greater application visibility.
- Detecting ATT&CK techniques & tactics for Linux / Windows.
- Understanding Linux / Windows Malware Persistence Methods.
- Detecting C2 network exfiltration and post-exploitation TTPs → use cases.

Copyright © Defensive Security All rights reserved.

MEET OUT TRAINER

LESZEK MIŚ

2017/18	BruCON
2018	OWASP Appsec US | FloCon USA
2018/19	Hack In The Box Dubai/Amsterdam/Singapore/Abu Dhabi
2019	44CON UK | Black Hat USA
2019	Confidence PL | PLNOG | Open Source Day PL | Secure PL | Advanced Threat Summit PL

Leszek Miś is the Founder of 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 DevOps, 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 2017/2018, Black Hat USA 2019, OWASP Appsec US 2018, FloCon USA 2018, Hack In The Box Dubai / Amsterdam / Singapore / Abu Dhabi 2018/2019, 44CON UK 2019, Confidence PL, PLNOG, Open Source Day PL, Secure PL, Advanced Threat Summit PL 2019.

Holds many certifications: OSCP, RHCA, RHCSS, Splunk Certified Architect.

His areas of interest include network "features" extraction, OS internals and forensics. Constantly tries to figure out what the AI/ML Network Security vendors try to sell. In free time he likes to break into "IoT world" just for fun.

Still learning hard every single day

Copyright © Defensive Security All rights reserved.

TRANING DELIVERY

DEFENSIVE SECURITY

Public with trainer

- Online
- Onsite

Private with trainer

- Online
- Onsite

During conferences

2020

- Hack in The Box
  - Amsterdam/ Singapore/ Abu Dhabi
- 44CON
  - London

Dedicated Webinars

- For organizations
- For Private cybersecurity specialists

“We share knowledge in various ways”

Copyright © Defensive Security All rights reserved.

TESTIMONIALS

It's been a while since I was so excited (like during #LockedShield2018).
Together with group of “sec-freaks” we had an opportunity to bring into play intensive scenarios and step into adversaries' shoes. I don’t remember when I exfiltration took away so much knowledge. Actually, is better to simply turn off computers. But try harder.”

Lukasz Chudzik
Cyber Security Advisor
GSA

“Thank You for the training. It was not only very informative but also eye opening. At first you start with thick book of well-prepared theory which you don’t have time to read because you are doing 25+ lab’s and get another 25 for homework.”

Participant of Hack In The Box Dubai 2018

“One of the best security exfiltration training so far! Lots of fun & learning! If you want to learn how hackers think and what kind of tooling they use - this is it!”

Participant of Black Hat 2019

“That was one of the most exciting Security trainings I have attended in the last few months. The scope of the training materials and Leszek’s approach are so great that I would like to spend more time to study the In & Out - Network Exfiltration Techniques.”

Participant of 44CON 2019

Copyright © Defensive Security All rights reserved.

TESTIMONIALS

"I wanted my team to experience something new, different ... I wanted SOC analysts to learn practical ways to bypass security and data exfiltration and learn to detect them and learn the techniques of attackers who could already break the security and work inside. And then Leszek appeared. We did not need a single coffee for three days! Leszek shared great knowledge with us in a very accessible way. Materials, pictures, scenarios - everything prepared and working. Thank you Leszek Miś! Highly recommend !!!"

Marcin Juszko
SOC Manager
PZU

"Thank you very much for delivering out a valuable workshop on data exfiltration techniques. The team is extremely impressed with the knowledge you present, as well as how easily you presented a very advanced topic. We have gained many useful cases that we will certainly use in practice. Thanks once again and respect!"

Wojciech Sielski
Chapter Lead Security
ING Tech

"Lots of hands-on labs. The trainer was very helpful and knowledgeable."

Participant
BruCON 2018

Copyright © Defensive Security All rights reserved.

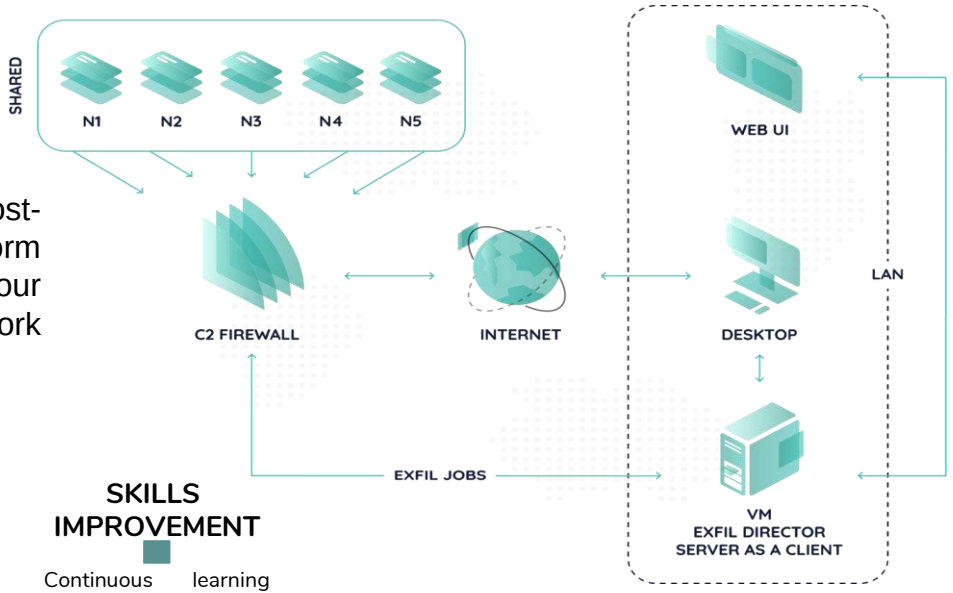
Services.

Closing gaps in your Network Security.

ADVERSARY SIMULATION

DEFENSIVE SECURITY

In & Out eXfiltration Platform 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.



INVESTMENT JUSTIFICATION

Test your SOC response on a real threat and demonstrate the value of IT Security investments to the Executive Board by simulating modern adversary behaviors

ON DEMAND VERIFICATION

Easy measurement and on-demand verification if your current network security solutions meet the compliance policy assumptions and work as expected

RED TEAM AUTOMATION

Out of the box adversary tools, techniques, and procedures delivered in the box allows for quickly deliver value and save time and money

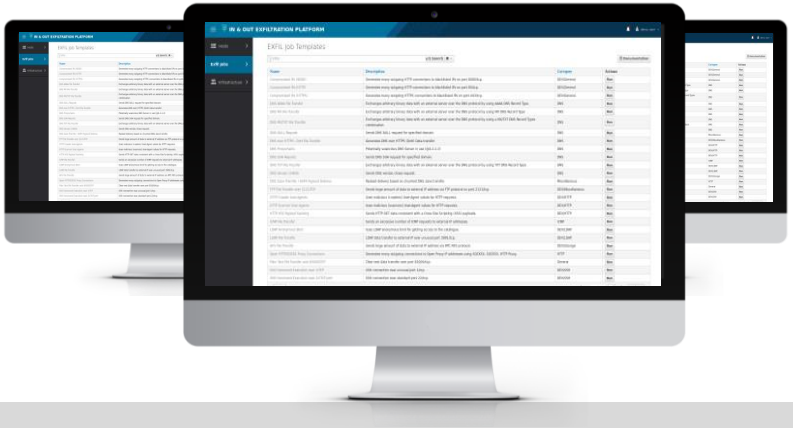
SKILLS IMPROVEMENT

Continuous learning about details of sophisticated network data exfiltration and lateral movement actions you have not been aware of before

Copyright © Defensive Security All rights reserved.

ADVERSARY SIMULATION

In & Out eXfiltration Platform



1. Ready to run in your multi-segment enterprise environment
2. Focuses on network events → generates multi-direction traffic: int2ext / int2dmz / dmz2ad / ad2mgmt / ad2ad / int2int etc.
3. Dedicated C2 Cloud Infrastructure included
4. Network Exfiltration and Post-Exploitation job definitions ready to run
5. In & Out Knowledge Base → stay up to date with new network TTPs
6. Useful for Red / Blue / Purple teams who want to validate network security posture
7. Risk and impact reporting
8. Provides metrics and mappings to MITRE ATT&CK Framework

Copyright © Defensive Security All rights reserved.

Thank you!

Don’t hesitate to contact us!

training@defensive-security.com