TRAINING NAME: Practical incident response

DURATION: 5 days

TRAINING OVERVIEW:

This hands-on training focuses on incident handling, from the first alert to the final report. Participants learn how to triage incidents, analyse the evidence, and work through the investigation steps a blue team analyst performs in a real case. The training starts with incident triage, where participants rate incidents, follow an escalation process, and complete analyst worksheets in a simulated incident queue. From there, the training moves into network traffic analysis, where participants use Wireshark, NetworkMiner, and tcpdump to investigate packet captures, including a compromised web server. They then evaluate how large language models (LLMs) and paid analysis services can support this work, and they build a script that uses an LLM to analyse malicious network connections.

Digital forensics is the next focus. Participants create disk images, carve deleted files, examine file metadata, and find hidden data through steganography. They analyse memory images with Volatility and Mimikatz, and recover Microsoft EFS-encrypted data from a disk image. The training ends with network detection and attack analysis using Suricata and Wazuh, a sample analysis of a ransomware infection, and a 360-degree attack analysis that ties together the evidence and techniques from the whole course.

An optional bonus module builds an Active Directory attack lab from scratch and examines attacks from three viewpoints: the attacker, the incident handler, and the administrator. Participants build Windows Server, Windows 11, Wazuh, and Kali Linux virtual machines, then work through AS-REP roasting and Kerberoasting using the LSHIFT methodology (Learn, Scan, Hack, identify hacking attempt, Fix it, Test the fix).

Most labs are guided, and some are self-study or trainer-moderated, with worked solutions provided for the incident triage exercise and the PCAP analysis tasks. Participants keep the lab virtual machines after the training so they can continue practicing at their own pace.

KEY LEARNING OUTCOMES:

- Explain cyber attack types, terminology, and the attacker's methods, including the Cyber Kill Chain and MITRE ATT&CK.
- Describe the incident response process and the NIST and ENISA frameworks.
- Triage security incidents by severity, follow an escalation process, and document findings with analyst worksheets.
- Respond to evolving incident updates in a live queue exercise.
- Capture and analyse network traffic with Wireshark, NetworkMiner, and tcpdump.
- Investigate PCAP files to determine what happened during an attack.
- Analyse traffic from a compromised web server and identify the attacker's actions.
- Detect network attacks with Suricata and Wazuh.
- Evaluate the use of LLMs and paid services for security analysis, and build a script that uses an LLM to analyse malicious connections.
- Create forensic disk images, analyse them, and handle evidence safely.
- Carve deleted files, examine file metadata, and detect hidden data through steganography.

- analyse memory images with Volatility and identify credentials exposed in memory with Mimikatz.
- Recover EFS-encrypted files using forensic and password recovery tools.
- analyse a ransomware sample and explain an attack from initial access to impact using a 360-degree view.

THIS TRAINING IS IDEAL FOR:

- SOC and NOC analysts who triage alerts and investigate incidents.
- Anyone interested in becoming a member of the blue team.
- Incident responders and digital forensic investigators.
- System and network administrators who want to move into monitoring and incident handling.

PREREQUISITES:

- Working knowledge of Windows and Linux operating systems.
- Basic understanding of TCP/IP networking and common protocols.
- Basic understanding of Active Directory, Kerberos, and NTLM (required for the bonus module).
- Hardware capable of running multiple virtual machines under Hyper-V (required for the bonus module).

TRAINING AGENDA:

Day 1: Understanding the attacker introduces cyber-attack types and terminology, the Blue/Red/Purple team concepts, the Lockheed Martin Cyber Kill Chain, and the zero trust model. Participants see demonstrations of common attacks, including man-in-the-middle, ARP spoofing, credential sniffing, SSL stripping, SQL injection, OS command injection, XSS, Log4Shell, misconfigured sudo privileges on Linux, and a malicious Office document. Each attack is linked to the evidence it leaves behind, so participants know what to look for as defenders.

Day 2: Incident response process covers the NIST incident handling process, the ENISA incident management guidance, and the MITRE ATT&CK framework. Participants learn how to rate incidents, follow an escalation process, and complete analyst worksheets. They then work through a live exercise using an incoming incident queue, responding to updates as the exercise progresses. A worked example solution is provided after the exercise.

Day 3: Incident detection: Network traffic starts with hands-on basics of Wireshark, NetworkMiner, and tcpdump (skip if already familiar). Participants then analyse two PCAP files in a self-study task, with worked solutions provided. The day continues with an analysis of traffic from a hacked web server, and with network detection using Suricata and Wazuh. Participants then explore analysis with AI (LLM) and paid services and build a script that uses an LLM to analyse malicious network connections. A challenge exercise on analysing malicious file infections is available if time permits.

Day 4: Digital forensics covers the forensic workflow. Participants start with disk imaging and basic analysis, which includes creating an image, analysing it, safely closing and removing the USB image, and analysing a hard disk. Next come file carving and metadata identification and analysis. The steganography lab uses spammimic and QuickStego. The memory analysis lab uses Volatility and Mimikatz on live memory. The Microsoft EFS decryption lab uses FTK Imager and Elcomsoft

Advanced EFS Password Recovery to extract data from an image, recover a password from the registry, and decrypt the protected files. The day ends with an analysis of an infected Windows memory image. Basic labs can be skipped by participants who already know them.

Day 5: End-to-end incident response scenario covers the analysis of already analysed pcap file, but this time with Suricata and Wazuh, then a collected ransomware sample will be analysed, followed by a 360-degree attack analysis. Participants follow the attack from initial access to impact, combine the evidence from network, host, and memory sources, and produce a final incident report.

Bonus module: AD attack scenarios (hacker, incident handler, and admin view) cover the following (this module is intro into a Hacking Active Directory: Detecting and Mitigating Compromises training) :

- Lab preparation: Participants prepare Hyper-V on Windows 10/11 and download the required files. They build Windows Server 2019 (with Windows Server 2022 and 2025 as optional builds), a Windows 11 client, and a Wazuh server on Ubuntu, including its components, UI connection, and networking. They install Wazuh agents on a domain controller and the Windows 11 client. They then set up the Kali Linux VM, including kerbrute and additional tools, IP address and networking, resolution, and SSH server. Final preparation includes generating users and Organizational Units in AD.
- AS-REP roasting: Participants learn how accounts with Kerberos pre-authentication disabled can be attacked and how to mitigate this. They scan the domain with Nmap, enumerate users, and perform password spraying. They extract and crack AS-REP hashes with hashcat, use NetExec to abuse the compromised account, identify the attack in logs and alerts, and apply and test the fix.
- Kerberoasting: Participants learn how service account tickets can be requested and cracked offline. They scan with Nmap, perform password spraying, identify kerberoastable accounts, request and crack service tickets with hashcat, and abuse the domain with NetExec. They identify the attack in logs and alerts, apply the fix, and test it.

ABOUT THE TRAINER:



Robert Petrunić works as a senior information security consultant in Eduron IS, the company dedicated to IT security education, penetration testing and computer forensics.

Robert is Microsoft certified trainer since 2002, EC-Council certified trainer since 2008 and (ISC)^2 certified trainer since 2014. Today, he lectures mostly hacking and security related courses for red teams and DFIR (Digital Forensics and Incident Response) related courses for blue team members. Since 2004, he worked primarily in the security field, and Microsoft acknowledged this in 2008 by assigning him the most valuable Microsoft professional recognition for nine years in a row.

For the last eighteen years, Robert has been working on programs related to ethical hacking and IT security awareness for systems administrators, developers, and IT security consultants. He is also often a lecturer at regional IT conferences.

Robert holds many industry certifications, including (ISC)^2 CISSP and CCSP, Offensive Security OSCP, OSCE and OSWP, EC-Council CPENT, CEH, CHFI, CND, and ECIH to name a few.