securITum

CERTIFICATE

OF PARTICIPATION IN THE TRAINING

TOP 10 WAZUH USE CASES – INCIDENT RESPONSE

2026

GRANTED TO:

Łukasz Bartos

DATE: 15/07/2026 **TRAINER:** Tomasz Turba **DURATION:** 2 hours

AGENDA

1. Blocking the attacker's IP address
2. Locking the user account
3. Host isolation
4. Malware quarantine
5. Killing reverse shell processes
6. Restarting the service
7. Notifications to the SOC team
8. Creating a service request
9. Adding IOC identifiers
10. Automatic incident triage

CPE/ECE POINTS: 2

SZKOLENIA.SECURITUM.PL