



SEKURAK.ACADEMY

# CERTYFIKAT

UCZESTNICTWA W SZKOLENIU SEKURAK.ACADEMY 2024

## WPROWADZENIE DO BEZPIECZEŃSTWA LINUX, CZĘŚĆ I (LOGI, PODSTAWY ANALIZY POWŁAMANIOWEJ)

DLA

**Marcin Kołodziejczyk**

DATA: 5.02.2024 R.

TRENER: Karol Szafrński

CZAS TRWANIA: 3.5 GODZINY

### AGENDA

#### LOGI I WIĘCEJ: WSZYSTKIE MOŻLIWE ŹRÓDŁA ZAPISANYCH ZDARZEŃ

- Syslog, journald i dmesg – co, gdzie i dlaczego jest logowane (lub nie)
- Gdzie i jak poza /var/log szukać logów usług i aplikacji
- Nie tylko historia Basha – przydatne ślady po użyciu narzędzi administracyjnych/programistycznych
- Auditd/SELinux – czego ciekawego można się dowiedzieć z ich logów
- Co się dzieje w kontenerach
- Metryki wydajności (CPU/RAM/IO) a włamanie i analiza powłamaniowa
- O prewencji – jak sensownie zbierać logi, jak silnie monitorować najważniejsze dla nas procesy i pliki

#### ANALIZA I WIZUALIZACJA AKTYWNOŚCI SIECIOWEJ

- Czy można zauważyć nietypowy ruch (eksfiltracja danych, komunikacja z C2), nie mając dużego i ciężkiego IDS-a
- Nie tylko tcpdump i Wireshark – garść mniej znanych narzędzi, które warto mieć pod ręką

#### PRZEGLĄD TECHNIK UKRYWANIA SIĘ STOSOWANYCH PRZEZ WŁAMYWACZY ORAZ SPOSOBY ICH WYKRYWANIA

- Fałszywe nazwy procesów, pozornie nieistniejące/ukryte pliki i inne triki
- Nieoczywiste lokalizacje złośliwych plików i ustawień, persystencja

PUNKTY CPE/ECE: 3.5

SZKOLENIA.SECURITUM.PL