

W04N Wydział Informatyki i Telekomunikacji

Kierunek: cyberbezpieczeństwo Specjalność: xxxx

Prowadzący pracę: XXXX

Jednostka organizacyjna: K34W04ND03 Katedra Telekomunikacji i Teleinformatyki

# KARTA PRACY DYPLOMOWEJ MAGISTERSKIEJ

**Temat pracy:**

(j. polski) Optymalizacja pracy analityka SOC poprzez agregację treści wielu źródeł typu ''threat intelligence''

(j. angielski) Optimization of SOC analyst workflow by aggregating content from multiple threat intelligence sources

**Aspekt badawczy:**

Przegląd literatury tematycznej dostepnej w czasopismach naukowych. Analiza kroków wykonywanych przez analityka SOC w celu oceny incydentu. Określenie metodyki analizy ryzyka. Przegląd istniejących rozwiązań informatycznych wspierających rozpoznanie incydentu. Określenie cech rekomendowanych narzędzia.

**Aspekt inżynierski:**

Analiza skuteczności (w tym mocnych stron i ograniczeń) przygotowanego narzędzia w stosunku do istniejących rozwiązań. Analiza SWOT.

**Zadania do wykonania:**

Określenie zestawu kryteriów efektywnej i skutecznej pracy analityka SOC. Przegląd istniejących rozwiązań informatycznych wspierających rozpoznanie incydentu. Określenie cech rekomendowanych narzędzia. Przygotowanie narzędzia agregującego dane z wielu źródeł typu threat intelligence.

**Literatura:**

MITRE - Ten Strategies of a World-Class Cybersecurity Operations Center, 2014

ENISA - How to set up CSIRT and SOC, Good practice guide, 2020 Recorded Future - The Threat Intelligence Handbook, 2019

**Temat zatwierdzony w dniu:** 23.02.2022

Podpis prowadzącego pracę Podpis opiekuna specjalności

**Akceptacja realizacji**

**Student:** xxxx **nr indeksu:** 021xxx190

Podpis studenta Data Podpis prowadzącego pracę