Implementacja Security Operations Center przy użyciu oprogramowania OpenSource

Temat pracy

Musi dotyczyć cyberbezpieczeństwa

`Implementacja Security Operations Center przy użyciu oprogramowania OpenSource`

Spis tresci

Krótko o tym jakie zagadnienia zamierzacie przedstawić w pracy.

- Triada CIA, koncept IAAAA
- Najbardziej prawdopodobne zagrożenia w organizacji
- Aktorzy i zagrożenia w cyberprzestrzeni
- Pojęcie Advanced Persistent Threat
- Software Sandboxing
- Blue Team
- Incident Response
- Insider threat
- Implementacja technologii
    - CTI
        - Cyber Threat Intelligence
    - HIPS / HIDS / NIDS / NIPS
        - Intrusion Detection / Protecion System
    - EDR / XDR
        - Endpoint detection and response
    - SIEM
        - Security information and event management
    - SOAR
        - Security Orchestration, Automation And Response
    - DLP
        - Data Loss Prevention
    - FIM
        - File Integrity Monitoring
    - Vulnerability Assessment and Management
- Retencja danych

Uzasadnienie tematu

I proponowanej zawartości pracy. Dlaczego chcecie o tym pisać, jaki będzie wkład praktyczny i czego będzie dotyczył - 1 akusz A4.

Dlaczego chcecie o tym pisać: W związku z obecną sytuacją na świecie oraz w cyberprzestrzeni jest to kluczowe aby każda organizacja w Polsce była w stanie obronić przed atakami, czy to wewnętrznymi czy zewnętrznymi. Każdy przedsiębiorca zdaje sobie również sprawę z jakimi kosztami wiąże się zaangażowanie w cyberbezpieczeństwo w jego organizacji.

Istnieją możliwości które pozwolą zabezpieczyć firmę przed zagrożeniami implemetując przy tym oprogramowania które posiadają otwarte źródło (OpenSource). Dzięki temu można zredukować większość kosztów związanymi z utrzymaniem oprogramowania (a są to bardzo duże koszty).

Jaki będzie wkład praktyczny i czego będzie dotyczył: Praca będzie opisywać jak wdrożyć dział Security Operations Center przy pomocy oprogramowań, które są dostępne za darmo i które można w takiej organizacji wdrożyć, ograniczając koszty. Znajdą się też takie informacje jak:

- jakie technologie, zasoby oraz umiejętności będą to tego potrzebne?
- jak zaprojektować taki dział, przepływ danych pomiędzy systemami i jak je zabezpieczyć?
- jakie procedury bezpieczeństwa w takim dziale należało by wdrożyć?
- jak poźniej taki dział przeszkolić i przygotować do dalszego rozwoju?