Cyber-MAR Piraeus Pilot / Final Event

Intrusion Detection and Situational Awareness

VTT Technical Research Centre of Finland Ltd.

Jarkko Kuusijärvi & Jukka Julku

December 16th, Piraeus, Greece

IDS & SA | Overview

- Security Onion based solution with Cyber-MAR extensions
  - Deployed in VTT’s Cyber-Range environment
  - Integrated with DIATEAM’s Cyber-Range using VPNs and CR and Module APIs

- IDS LogMon Module:
  - Signature-based network intrusion detection (Suricata)
  - Network security monitoring (Zeek NSM)
  - Host-based intrusion detection (Wazuh)
  - SSL Inspection proxy

IDS & SA | Overview (cont.)

- Expert Situational Awareness Module
  - Management of generated alerts and events (Squert)
  - Displaying monitoring data gathered from the network and hosts (Kibana)
  - Cyber-MAR extensions, e.g., visualization of Prediction Engine output

- High-Level Situational Awareness Module
  - Visualization of cyber security risk level
  - Security Metrics Model, a filtered high-level view of selected system

IDS & SA | IT Network

- The intrusion detection and monitoring system in organization’s IT network
  - Three network probes in routes between different network segments
  - Host-based detection on two of the workers’ machines
  - SSL inspection proxy for outgoing HTTPS traffic
- Indicators of Compromise for the attack
  - Threat Intelligence downloaded from the community over MISP
    - IoCs related to the attack, e.g., malicious IP addresses, file hashes
  - Organization specific rules for monitoring and logging normal traffic
    - E.g., external VPN connections, remote management

IDS & SA | OT Network

- The intrusion detection and monitoring system in organization’s OT network
  - One network probe
  - Host-based detection on three machines, but not on the PCLs
    - E.g., SCADA supervision server, machine used to develop and maintain the PLCs
- Indicators of Compromise for the attack
  - Same IoCs as for the IT network
  - Organization specific rules for monitor and logging PLC management
    - E.g., PLC start, stop, reprogramming

Pilot Execution

Cyber MAR

🌐 www.Cyber-MAR.eu

Cyber_MAR

▷ Cyber-MAR EU Project

in Cyber-MAR

✉ info@lists.Cyber-MAR.eu

THANK YOU FOR YOUR ATTENTION

VTT

VTT Technical Research Centre of Finland Ltd.

✉ firstname.lastname@vtt.fi

This project has received funding from the European Union’s horizon 2020 research and innovation programme under grant agreement No. 833389