

Yael Snear CV

yaelsnear@gmail.com | 054-4402840 Kfar Yona

Experience

IDF - intelligence corps:

2021 – Today: SOC team leader

- Managing and training a team of analysts
- Managing network security incidents from identification to resolution
- Cooperating with 3rd party providers, tech consultants and Cyber security agencies
- Project managing including research, comparison, testing, POC and implementation of suitable security products and tools for the **IDF Internet network and cloud infrastructure - Azure**

2019 – 2021: Security Analyst – SOC team

- Instructor in Cyber Analyst course: introduction to computer networking
- Monitoring the IDF internet and cloud networks in aspects of cyber security threats
- Operating different security systems and implementing new policies
- Threat intelligence – online researching, implementing proactive rules to improve detection of advanced threats

Skills

- **Azure-**
 - **MCAS-** rules creation, event handling and monitoring
 - **Sentinel-** monitoring
 - Threat hunting via **KQL queries**
 - **DLP-** environment design and monitoring
 - **ATP-** monitoring
- **Network traffic analysis (Security)** - Using Wireshark, Solera (Blue Coat)
- **Fortinet** – operating **FortiGate FW**, network monitoring with **Forti Analyzer**
- **EPO (McAfee)** - rules distribution, Maintenance, and monitoring, specializing in **DLP**
- **IronPort (Cisco)** - Monitoring and identifying malicious emails + Policy management
- **Sandbox** - reports analytics of **FireEye** Sandbox (EX+NX), **Forti** Sandbox and **Symantec Blue Coat** Malware Analysis Sandbox.
- **SIEM MicroFocus ArcSight** - rules creation, monitoring and maintenance

Education

2021 - Microsoft Azure Security Technologies (**AZ-500**) Certificate by BeyondCloud

2021 - Microsoft Azure Administrator (AZ-104) Certificate by BeyondCloud

2021 - Microsoft Azure Fundamentals (AZ-900) Certificate by BeyondCloud

2020 - Introduction to Sentinel in Azure cloud environment

2019 - Security Analyst - IDF

High School (2016-2019) – with honor