102779-ITN-7s-E-2019
Senior Technical Cyber Security (IT/OT) Engineer

Holds a B. Sc. in Electrical & Communication Engineering and has over 2 years experience as ICS/OT Cybersecurity Engineer with a proven track record in identifying and mitigating cyber threats.

PERSONAL DATA

Nationality	:	Egyptian
Gender	:	Male
Residence	:	Cairo

EDUCATION

: B. Sc. in Electrical & Communication Engineering, Mansoura High Institute of Engineering and Technology, 2019

LANGUAGES

Arabic	:	Native Language
English	:	Excellent

COMPUTER SKILLS

: Windows, MS Office, Internet

TRAINING COURSES AND CERTIFICATIONS

: Computer Hacking Forensic Investigator (CHFI v10) ECC8493150276.
: The Red Hat Certified System Administrator (EX200) Exam 220-140-974.
: Cyber Defense Engineer Internship, WE INNOVATE (Jul. – Nov. 2023).
: NTI Digital Youth Initiative (4 months) (540 hours), National Telecommunications Institute (Sep. 2022 – Jan. 2023).
: 3 Month Intensive Code Camp / System Administration Track, Information Technology Institute (ITI) (Apr. – Jul. 2022).

CHRONOLOGICAL EXPERIENCE RECORD

Dates : From Feb. 2024 till now
Employer : RATP Mobility Cairo
Job title : Senior Technical Cyber Security (IT/OT) Engineer
Job Description :

- Enhancing Cybersecurity for (IT/OT) by Generate risk assessment and create a timeline with short-term and long-term goals against IEC 62443.
- Develop and test ICS/OT-specific incident response plans.
- Reviewing the configurations for the firewalls (FortiGate).

- Participating in security awareness programs and training to educate employees for (IT/OT) environments.
- Ensure Periodic review of systems, network, Switches, and security solutions logs.
- Reviewing administrators reports and taking the required actions regarding any suspicious event.
- Monitoring Endpoint devices using SentinalOne XDR, ESET Antivirus solution and Intune for all 15 subsidiaries.
- Monitoring Proofpoint Email Protection gateway for any phishing, BEC and taken over outlook accounts attempt over all subsidiaries.
- Checking the latest threats and practices to address security exposures and threats (Threat Intelligence).
- Applying Information Security Policies.
- Incidents Management (incident handling, response and investigation).
- Maintained comprehensive documentation of security architectures, configurations, incidents, and response actions. Generated regular reports on security posture and incidents.
- Create playbooks for different incidents, and (Firewalls, Switches, Access points) baselines.

Dates : From Jul. 2023 till Feb. 2024
Employer : RATP Mobility Cairo
Job title : Cyber Security ICS/OT SOC T2 Engineer
Job Description :

- Starting building information security team and training the hired staff.
- Team Leader for 5 members of SOC T1 and handled escalated incidents from T1.
- Analyze alerts from intrusion detection systems (IDS) and security information and event management (SIEM) systems.
- Applying incidents management process and procedures.
- Document and report control failures, gaps, and finding to stakeholders.
- Conduct forensic analysis of ICS/OT systems in the event of a security breach.

Dates : From Jan. 2023 till Jul. 2023
Employer : RATP Mobility Cairo
Job title : Cyber Security ICS/OT SOC T1 Engineer
Job Description :

- Continuous Monitoring for OT/IT environments 24x7 bases.
- Security Threats Detection within network, servers & endpoint devices.
- Security Incident response.

Dates : From Jan. 2022 till Jan. 2023
Employer : Telecom Egypt
Job title : Network Maintenance Engineer
Job Description :

- Oversee the physical installation of new devices (Routers, Servers, and ODFs) from various vendors.
- Manage, track, and collaborate with problem and escalation processes.
- Monitor the devices performance and the temperature, diagnose and resolve network problems.

- Investigate the sites and devices using multiple vectors and report monthly to the lead engineer.
- Accept new tickets using the ATTS ticketing system and move them to different teams and sections.
- Manage onsite technical support for Technicians and Engineers.

Skills:

- Incident Response & Blue Teaming:
  - Windows, Network and Digital Forensics Understand and analyze evidence to investigate cyberattacks.
  - Incident response: Effectively responding to cyberattacks and minimizing their impact.
  - Static, Dynamic Malware Analysis.
  - Threat Hunting.
  - Open-Source Cyber Intelligence.
- Cyberops / Network security:
  - Device Logging and Monitoring Aggregation and Correlation experience (SIEM).
  - Experience with IP networking, networking protocols, IPsec, PKI, VPNs, firewalls, endpoint security.
  - Familiarity with Linux, Windows, and other network operating systems.
- ICS/OT Cyber Security:
  - Managing IT/OT firewalls and IDS/IPS.
  - Gap Analysis (against IEC 62443, NIST CSF).
  - Risk Assessment as per international standard ISO 27005.
  - Vulnerability identification (using MITRE ATT&CK).
  - Secure Network Architecture (Purdue Model).
- Nozomi IDS workshop: configuration of industrial IDS, Monitoring.
- Fortinet workshop: ICS Firewall configuration.
- Linux system administration: Bash, Apache, Nginx, ISM, Firewall management, SELinux, Containers.