100310-ITN-467s-E-2015
Cyber Security Respond & Recover Team Leader

Holds a B. Sc. in Mechatronics Engineering and has over 9 years experience working in cyber security field.

PERSONAL DATA

Nationality	:	Egyptian
Birth Date	:	15/10/1991
Gender	:	Male
Marital Status	:	Married
Residence	:	Giza, Cairo

EDUCATION

: B. Sc. in Mechatronics Engineering, Higher Technological Institute, 2015
: Secondary Education: El Mobtadian Language School, Mounira, Cairo

LANGUAGES

Arabic	:	Native Language
English	:	Excellent

COMPUTER SKILLS

: Windows, MS Office, Internet

TRAINING COURSES AND CERTIFICATIONS

: American Chamber: Soft Skills Business Package.
: Microsoft Windows.
: Linux/Unix based Systems.
: Network+.
: Security+.
: Ethical Hacking.
: Security Analysis.
: Vulnerability Assessment.
: IPS "XGS".
: SIEM "Qradar".
: Web Applications Dynamic Scanning "App Scan".
: IRP "Resilient".
: Security Monitoring.

: Incident Investigations.
: Threat Hunting.
: Incident Response.
: Incident Handling.
: SOC GAP Assessment.
: SOC Building.
: Procedures & Process building.
: SOAR.
: ICS Security.
: OT Security.
: Risk Assessment.
: Risk Management.

CHRONOLOGICAL EXPERIENCE RECORD

Dates : From May 2019 till now
Employer : Information Technology Solutions
Job title : Cyber Security Respond & Recover Team Leader

Dates : From Jan. 2017 till May 2019
Employer : Information Technology Solutions
Job title : Security Intelligence Specialist

Dates : From Apr. 2015 till Jan. 2017
Employer : Information Technology Solutions
Job title : Security Service Integrator

Dates : From Jan. 2015 till Apr. 2015
Employer : Ceramica Cleopatra Group
Job title : IT Help Desk

Skills:

- Developing Schedules.
- Time Estimating.
- Creating Charts and Schedules.
- Managing Risks and Issues.
- Monitoring and Reporting Progress.
- Team Leadership.
- Controlling Quality.
- Improve team skills.
- Apply KPIs.
- Motivation & feedback sessions.

Projects:

- SIEM Qradar Implementations (9 Engagements): Perform Application installation, Adding & Tuning sources, Creating & Tuning rules/usecases.
- Appscan Implementations (2 Engagements): Perform Application Installation, Create Scanning Templates, generating Reports and Report Analysis.
- IPS XGS (1 Engagement): Installing Physical connection and Design Architecture, Adding and Tuning Network and Rules Objects.
- IRP Resilient (4 Engagements): Perform Application Installation, Create Incident response Procedures, create work flows, Create KPIs and SLAs, Perform Integrations with other systems.
- SOC Gap Analysis & SOC Building (3 Engagements): Participate in SOC Gap Analysis based on metrics and deliver documents and work shop sessions, Participate in SOC Building (Work Orchestration, Validation of Information, Setting KPIs for SOC Team and Reporting Matrix) finally Delivering Tailored Incident Response Procedures and work flows based on environment variables.
- Incident Handling Drill (1 Engagement): Develop Incident handling drill for customer in order to test SOC & Incident Response Team Capabilities and provide document with scenarios, Incident handling drill was held as tabletop exercise & a full live demonstration with injected data.
- Risk Assessment (1 Engagement): Practice IT risk assessment based on CIS & NIST standards providing qualitative assessment for business and IT with detailed risk register containing overall risk score.

This experience was gained in different industries (Banking, Oil & Gas, Telecoms, SMEs …etc.).