Abdelrahman Esmail, Threat Detection Engineer

Cairo, Egypt, 01205520646, abdelrahman.mohamed.esmail@gmail.com

PROFILE

Threat Researcher with 5+ years' experience in pre-sales, threat analysis, and network signature rules. Proven track record in managing large-scale projects from both sales and R&D perspectives.

EMPLOYMENT HISTORY

May 2023 — Present

Senior Threat Detection Engineer, Trend Micro

Cairo

- Developed, designed, and refactored threat models that correlated with hybrid, on-premise, container, and cloud environments to give 360 visibility for customers.
- Tracked new APT group's activities on Kibana and Splunk to track zero-day attacks and exploited in the wild CVEs to provide customer coverage in less than 24 hours.
- Built a new XDR telemetry schema for container environments which helped to co-relate container activities from K8s, Openshift, and ECS orchestrations with other cloud, endpoint, and workload activities.
- Developed tools to help in daily testing for regression, FP, and unit testing with Atomic-Red-Script.

Dec 2022 — Apr 2023

Senior Threat Detection and Response, Trend Micro

Cairo

- Led the initiative to redesign, optimize, and maintain vulnerability network signature rules and decoders, resulting in a 20% performance improvement and a 35% reduction in false positives
- Led the weekly end-to-end release process of signatures to the customers.
- Managed customer escalations related to Deep Security IPS signatures for security incidents, and false positives/negatives with the same weekly sprint.
- Conducted vulnerability research and performed simulations for IPS signatures, addressing undisclosed items from ZDI and other TrendLabs, resulting in IPS coverage for 2 weeks before the vendor's official patch.

Jun 2020 — Nov 2022

Threat Detection and Response, Trend Micro

Cairo

- Desgined and fine-tuned sophisticated network signature rules which need more research work with new network protocols for C1WS.
- Vulnerability research, verification, and reproduction for n-day, 0 days, and undisclosed items from TrendLabs.
- Administered Customer issues and inquiries on an average of 4 working days.

Dec 2018 — Jun 2020

Systems Engineer, Trend Micro

GCC

- Co-ordinated the GGC region, mainly to cover UAE, and Saudi Arabia as systems engineer with more than 7.5 million deal.
- Led the development and execution of health check program, resulting in a 15% increase in customer retention and $3M in new revenue from cross-selling Trend Micro products and services.

EDUCATION

Sep 2014 — Jul 2018

Bachelor of Computer and Information Science, Ain Shams University

Cairo

Graduated with B with score 73.81%

SKILLS

- Research
- Continuous Delivery
- Analytics
- Cyber Risk
- Threat Detection
- Customer Service
- Ability to Multitask
- Threat Hunting
- TCP/IP
- Vulnerability Signatures
- Snort
- C++
- C
- Python
- Purple Team
- Windows/Linux

Threat Analysis
Detection Engineer
Container
K8S
AWS
Azure
CEH
OSCP
OWASP
globally distributed team
Research initiatives
Suricata
Wireshark
HTTP
IDS
IPS
Exploitation

LANGUAGES

Arabic — Native speaker
English — C1

INTERNSHIPS

Oct 2018 — Nov 2024

Trend Micro Certification program in IT Security, Trend Micro — Cairo

- Gained practical, hands-on experience and product certification for 6 Trend Micro products which cover hybrid cloud security, network defense, and endpoint protection solutions.
- Applied knowledge in real-world scenarios, Collaborated with a team, completing 2 deals projects within 1-month deadlines.

Dec 2017 — Apr 2018

Cybersecurity Specialization, University of Maryland — Remote

- Graduated of rigorous 2-month cyber security Specialization program. Also obtained of certificates for usability, cryptography, web pen-test.
- Built a project to applied Cryptanalysis techniques for +10 cryptography algorithms.

COURSES

Sep 2021 — Nov 2024
Associate AWS Certified Developer, Amazon Web Services

Jul 2021 — Jul 2024
Amazon Web Services Solutions Architect Associate, Amazon Web Services

Feb 2021 — Feb 2024
Amazon Web Services SysOps Administrator - Associate, Amazon Web Services

Dec 2020
CNSS Certified Network , The Institute of Company Secretaries of India

Mar 2018
Cybersecurity Specialisation, University of Maryland, College Park