# Abdelrahman Esmail

## Sr. Engineer-Threat Research

Elsalam, Cairo 11788 | 01205520646
abdelrahman.mohamed.esmail@gmail.com | https://soom3a.github.io/Blogs/

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

## Work Experience

**Sr. Threat Detection and Response** Apr 2023 – Present
Trend Micro | Cairo, Egypt

- 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.

**Sr.Threat Detection and Response** Jan 2023 – Mar 2023
Trend Micro | Cairo, Egypt

- 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 Trend-labs, resulting in IPS coverage for 2 weeks before the vendor's official patch.

**Threat Detection and Response** May 2020 – Mar 2023
Trend Micro | Cairo, Egypt

- Designed 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 Trend-labs.

- Administered Customer issues and inquiries on an average of 4 working days.

**Technical Sales** Dec 2018 – May 2020
Trend Micro | Riyadh, Saudi Arabia

- Assist customers' technical requests and take care of any technical issues
- Build strong customer relationships, especially with key customer stakeholders and sponsors
- Provide technical support for customers to support per-sales and post-sales processes
- Address all product-related queries on time
- Train customers to use products effectively
- Report on product performance
- Identify solutions to reduce support costs
- Analyze customers' needs and suggest upgrades or additional features to meet their requirements
- Establish best practices
- Always strive to provide exceptional customer experience
- Manage customer expectation and lead them to customer satisfaction
- Make sure all deliverables arrive in good order, on time, and fulfill customers' requirements
- Take initiatives in identifying growth opportunities
- Collaborate with our team to achieve sustainable growth
- Identify customer security and connectivity requirements, and propose Trend Micro solutions to address these needs. Solutions include but are not limited to Data-center, Network, and User Security.
- Confirms Trend Micro's products meet the prospect's requirements and assist sales in technical qualification during the qualifying process.
- Work with a customer's technical contacts during evaluation/demonstration periods, respond to their technical issues/questions and act as the liaison between the customer and engineering as well as product management and marketing.
- Understanding customer IT/Security infrastructure and business requirement
  Strategic Solution selling
- Solution Demonstrations and Proof of Concepts
- Business Solution Proposals, RFI/RFP specification preparations
  Having Strong understanding of Trend Micro portfolio, including but not limited to Deep Security, DDI, DDEI, DDAN, OfficeScan, SMEX, SMLD, IMSVA, IWSVA, CAS and HES.

**Trainee** Oct 2018 – Nov 2018
Trend Micro | Cairo, Egypt

- Graduate of rigorous 8-week Trend Micro Certified Program in IT security.
- Gained practical, hands-on experience and product certification with Trend Micro's market-leading hybrid cloud security, network defense and endpoint protection solutions.

- Developed team and presentation skills, and deeper knowledge of networking, virtualization, Advanced persistent threat and cloud computing

**Student** Sep 2014 – Jun 2018
Faculty of Computer and Information Science, Ain Shams University | Cairo, Egypt

## Projects

**Recomendation Scan Automation** Jan 2022 – May 2022

Update legacy code to Python3 and OSs infrastructure, to be fully automated for windows update and deal with latest Deep security installation update with 1 click. the cycle reduced from ~7 hours to less than 1 hour)

**Atomic Red Script Automation** Feb 2023 – May 2023

Build a fully regression automation to test Trend Micro container security rules against malicious attacks on different Cloud Providers (AWS-EKS, AWS-ECS, GCP, Azure, OpenStack)

**CISA KEV Parity Check** Mar 2024 – Sep 2024

A report contains the full information for Vulnerability listed in CISA KEV with Trend Micro current coverage for all possible solutions. The result will be pdf contains Trend Micro current score coverage and KEVs missing with available POCs/exploitation with old cases.

## Core Skills

Customer Service, Intrusion Detection, Host Intrusion Prevention, Kubernet, Wireshark, TCP/IP, OWASP, Vulnerability Signatures, falco , Snort, Suricata, CEH, OSCP, Amazon Web Services (AWS), Microsoft Azure, Amazon ECS, Amazon EKS, Kubernetes, Presentations, Network Traffic Analysis, Malware Analysis, Reverse Engineering , Static Analysis, Dynamic Analysis, Mitre, Sigma, Yara, Linux, Windows Server, Azure

## Education

**Faculty of Computer and Information Science Ain Shams** Jan 2014 – Jun 2018
Bachelor of computer science

**Mostafa Kamel** Jan 2011 – Jan 2013
**high school** | Mathematics Section.

## Languages

Arabic (NATIVE), English (PROFESSIONAL)

## Awards

**ZDI Acknowledgment** Feb 2024
Trend Micro ZDI

- ZDI Acknowledgment for tracking the Water Hydra Targets Traders on SmartScreen Zero-Day.
- ZDI Acknowledgment for tracking campaigns "Void Banshee Targets Windows Users Through Zombie Internet Explorer in Zero-Day".

**Trend Micro Internal CTF - Technical Day** Jan 2023
Trend Micro
2nd place in Trend Micro Capture the flag internal competition for Trend Micro employees (R&D, System Engineers).

**Employee of The Year Deep Security Labs** Dec 2022
Trend Micro
The Best Trend Micro Threat Researcher for implementing and upgrade from legacy systems

**Cyber Talents Egypt CTF** May 2018
Cyber Talents
5th place in Egypt Capture the flag competition under team name Code4Duty.

**Cyber Talents Egypt CTF** Apr 2017
Cyber Talents
9th place in Egypt Capture the flag competition under team name Flag3nters.

## Certificates

**McKinsey Forward Program**
McKinsey & Company
**AWS Certified Developer – Associate** Sep 2024
Amazon Web Services (AWS)
**CNSS Certified Network - ICSI**
ICSI
**AZ-301 Microsoft Azure Architect Design** Apr 2022
Microsoft
**Microsoft Certified: Azure Solutions Architect Expert** Apr 2022
Microsoft

**AZ-300 Microsoft Azure Architect Technologies** Mar 2022
Microsoft
**Amazon Web Services SysOps Administrator - Associate** Dec 2022
Amazon Web Services (AWS)
**Amazon Web Services Solutions Architect Associate** May 2022
Amazon Web Services (AWS)
**Apex One Certified Master** May 2021
Trend Micro
**Deep Discovery Advanced Threat Detection 2.1 Certified Professional** Nov 2020
Trend Micro
**OfficeScan XG Certified Professional** Nov 2020
Trend Micro
**XGen Endpoint Launch Essentials for Technical Sales** Nov 2020
Trend Micro
**Advanced Threat Centric Education – Intermediate v3**
Trend Micro
**Deep Security 11 Certified Professional** Oct 2020
Trend Micro
**Hybrid Cloud Security Essentials for Technical Sales** Jan 2021
Trend Micro
**Cybersecurity Specialization**
Coursera
**Cybersecurity Specialization**
University of Maryland, College Park
**Cryptography**
Coursera
**Hardware Security**
Coursera
**Software Security**
Coursera

## Publications

**Silent Intrusions: Godzilla Fileless Backdoors Targeting Atlassian Confluence** Jan 2024
TrendMicro

**Cryptojacking via CVE-2023-22527: Dissecting a Full-Scale Cryptomining Ecosystem** Jan 2024
TrendMicro

**CVE-2024-38112: Void Banshee Targets Windows Users Through Zombie Internet Explorer in Zero-Day Attacks** Jan 2024
TrendMicro

**CVE-2024-21412: Water Hydra Targets Traders With Microsoft Defender SmartScreen Zero-Day** Jan 2024
TrendMicro

## Interests

Capture The Flag, Reading, Problem Solving, APT Tracking, Threat Intelligence , Coding