Ahmed Fathi Mahmoud Elesawi

Network Security Engineer

Brief

Ambitious individual with proven leadership skills, adept at problem-solving, prioritization and multitasking in challenging environments.
Demonstrated expertise in network security with a strong foundation in technology.
Eager to apply my knowledge and skills to overcome diverse challenges.

Personal Information

Birth Date: *16-Sep-1995*
Residence: *Cairo, Egypt*
Military Status: *Served*

Contact Information

Mobile: *01158373746*
Email: *ahmed@elesawi.com*
LinkedIn*: linkedin.com/in/elesawi*

Education

Bachelor of Engineering – BE
Marg High Institute for Engineering and Technology | 2013 – 2018

Field of Study: *Electrical, Electronics and Communications Engineering*
Grade: Very Good (**2.92 GPA**)
Project: *Robotic Arm with Computer Vision, showcasing proficiency in emerging technologies and project management. (**Excellent**)*

Experience

Network Security Engineer
Banque Misr | 07/2024 – Current

- ***Firewall Rule Management:***
  - *Administer and maintain firewall policies across multiple platforms, including **Palo-Alto** firewall, **FortiGate**, and **Cisco ASA**.*
  - *Ensure firewall rules are correctly configured, optimized, and aligned with security policies, improving traffic flow and reducing network vulnerabilities.*
  - *Applied expertise in rule management to prevent unauthorized access while minimizing network disruptions.*
  - *Worked closely with other teams to regularly update rulesets to reflect changes in security policies.*
- ***Access Control Implementation:***
  - *Handle requests for new access according to InfoSec approvals, ensuring secure access is granted to the appropriate users or systems.*
  - *Regularly coordinate with internal teams to verify the need for access, balancing business functionality with security compliance.*
- ***VPN Configuration and Management:***
  - *Configure, maintain, and troubleshoot site-to-site and SSL VPNs to ensure secure communications between internal systems and external partners.*
  - *Ensured seamless connectivity by promptly resolving VPN issues, enabling uninterrupted operations for remote users and business partners.*
- ***Palo Alto Panorama Management:***
  - *Utilize **Palo Alto Panorama** to centralize firewall management, streamline security policy updates, and enhance visibility across the network.*

- ***FortiManager and FortiAnalyzer Administration:***
  - *Manage the **FortiManager** for centralized firewall management and use **FortiAnalyzer** for log analysis, troubleshooting, and reporting, improving incident response times.*
  - *Leveraged **FortiAnalyzer** to proactively detect anomalies, helping to identify and respond to potential security threats quickly*
- ***Automation:***
  - *Developed Python scripts to automate firewall rule management and streamline bulk editing of firewall configurations, increasing efficiency and reducing manual errors.*

Network Security Engineer

Raya Information Technology | 07/2023 – 06/2024

- ***Key Role in Critical Infrastructure:***
  - *Serve as a resident network security engineer at **Banque Misr**, playing a pivotal role in ensuring the security and integrity of critical banking infrastructure.*
  - *Deploy and configure a range of security appliances, including **FortiGate**, **FortiManager**, and **FortiAnalyzer** to safeguard against cyber threats and vulnerabilities.*
- ***Expertise in Next-Generation Firewalls:***
  - *Manage and maintain **Palo-Alt** Firewall with **Panorama** and **FortiGate**, ensuring robust protection against advanced threats and unauthorized access.*
  - *Configure and optimize site-to-site VPNs and SSL VPNs, enabling secure communication channels for remote access and inter-office connectivity.*
- ***Proactive Security Measures:***
  - *Implement and update security policies to align with industry best practices and regulatory requirements, bolstering the overall security posture of the organization.*
  - *Play a key role in the migration of existing firewall configurations, demonstrating adaptability and meticulous attention to details.*
- ***Troubleshooting and Incident Response:***
  - *Identify and troubleshoot issues related to VPN connectivity, ensuring seamless and uninterrupted access for users and stakeholders.*
  - *Collaborate with cross-functional teams to investigate and mitigate security incidents, minimizing the impact of potential breaches and intrusions.*
- ***Continuous Improvement and Collaboration:***
  - *Contribute to ongoing efforts to enhance network security through the evaluation and adoption of new technologies, methodologies and best practices.*
  - *Collaborate closely with internal teams and external partners to address emerging threats and vulnerabilities, fostering a culture of proactive security awareness and response.*

Instructor (Part Time)

NTI - National Telecommunication Institute | 06/2023 – Current

- *Conduct lectures and hands-on training sessions for cybersecurity students at NTI, operating under the supervision of the Ministry of Communications.*
- *Utilize innovative teaching methods and hands-on labs to create an engaging and effective learning experience for students.*
- ***EC-Council Certified Ethical Hacking:***
  - *Deliver comprehensive courses on ethical hacking, covering topics such as penetration testing, vulnerability assessment, and ethical hacking methodologies.*
  - *Instruct students on advanced hacking techniques, including footprinting, reconnaissance, and exploit development, to enhance their understanding of offensive security practices.*
  - *Incorporate real-world case studies and practical exercises to provide students with practical skills and prepare them for industry certification exams.*

- *Collaborate with students to develop ethical hacking projects, fostering creativity and problem-solving skills in cybersecurity.*

- ***Cisco CyberOps Associate:***
  - *Lead courses focused on Security Operations Center (SOC) operations, including network intrusion analysis, incident response, and threat intelligence integration.*
  - *Provide hands-on training on SOC tools and technologies, such as SIEM platforms (**Security Onion**), threat hunting tools, and incident response platforms.*
  - *Guide students through simulated cyber-attack scenarios, enabling them to analyze and respond to security incidents in a SOC environment.*
  - *Foster collaboration among students by organizing team-based exercises and SOC simulations, promoting teamwork and critical thinking skills essential for SOC analysts.*

Instructor (Part Time)

YAT learning Centers | 06/2023 – Current

- *Conducted engaging lectures and in-person training sessions for cybersecurity students enrolled in the **Digital Egypt Cubs Initiative (DECI)**, operating under the supervision of the Ministry of Communications and in collaboration with **Udacity** platform.*
- *Developed and implemented engaging activities and exercises suitable for younger learners to reinforce cybersecurity principles and practices.*
- *Facilitated simulations adapted to the age of the groups to provide practical experience in real-world cybersecurity scenarios.*

Instructor (Part Time)

MASA for Training and Consulting at Thebes Academy | 07/2023 – 09/2023

- *Conduct lectures and hands-on training sessions for cybersecurity students at **Thebes Academy**.*
- *Utilize innovative teaching methods and hands-on labs to create an engaging and effective learning experience for students.*
- *Instructed students on footprinting, reconnaissance, and exploit development, enhancing their understanding of offensive security practices.*
- *Integrated real-world case studies and practical exercises to equip students with practical skills and prepare them for industry certification exams.*

Network Security Engineer Trainee

BARQ Systems | 05/2023 – 06/2023

- ***Comprehensive Shadowing Experience:***
  - *Gained invaluable insight into network security operations by shadowing experienced professionals.*
  - *Observed and participated in the installation, configuration, and troubleshooting of key security technologies, including **APEX One**, **FortiGate**, **FortiManager**, and **F5 LTM** & **ASM**.*
- ***Hands-on Learning:***
  - *Engaged in practical training sessions to develop proficiency in deploying and managing security solutions.*
  - *Acquired practical skills in configuring and troubleshooting security appliances, enhancing technical capabilities in network security.*
- ***Collaborative Environment:***
  - *Worked closely with team members to address real-world challenges and apply theoretical knowledge to practical scenarios.*
  - *Participated in team discussions and problem-solving sessions, contributing to a collaborative learning environment.*

Electrical Site Engineer

ECS - Energy and Contracting Solutions, Cairo Business Park Project | 07/2021 – 01/2023

- *Experienced Electrical Site Engineer with a proven track record in executing and overseeing electrical works at construction sites. Skilled in resource management, project planning, and ensuring quality control. Adept at providing technical support and collaborating with cross-functional teams for successful project execution.*
- ***Implementation and Oversight:***
  - *Execute and supervise various electrical works at the construction site.*
  - *Allocate and manage resources for workforce, materials, and equipment.*
- ***Planning and Analysis:***
  - *Plan construction methodologies and recommend optimal options.*
  - *Interpret construction drawings and ensure compliance with standards.*
- ***Technical Support:***
  - *Provide engineering support to electrical workgroups at the site.*
  - *Collaborate with mechanical and civil groups for seamless project execution.*
- ***Project Management:***
  - *Plan and execute electrical works, aligning with project timelines.*
  - *Manage resources efficiently to support project goals.*
- ***Quality Control:***
  - *Implement and verify electrical works to ensure compliance with quality standards.*
  - *Ensure adherence to construction drawings and relevant specifications.*

Courses and Training

Modern Defensive Security Solutions

NTI, Digital Egypt Youth Initiative| 02/2023 – 05/2023

- *Developed proficiency in various security appliances, including **ASA**, **FortiGate**, **Forti-Manager**, **Forti-Analyzer**, **Forti-SIEM**, **FORTI-Web**, **Palo-Alto** Firewall and **Sophos** Firewall, through hands-on labs and real-world scenarios.*
- *Developed my Soft skills such as communication and team working, through various scenarios and situations.*

Network Attacks and Mitigations

NTI | 09/2022

- ***Learned and Applied:***
  - *Foundational security concepts, principles, and best practices.*
  - *Network intrusion analysis techniques for threat detection*
  - *Endpoint threat analysis and computer forensics skills.*
  - *Understanding of security policies, procedures, and compliance.*
  - *Security monitoring practices for real*
  - *Incident response strategies for effective mitigation.*
  - *Operations of a Security Operations Center (SOC).*
  - *Visualization of security data for enhanced decision*
  - *Integration of threat intelligence into security operations.*
- ***Developed Skills:***
  - *Threat detection and analysis within network traffic.*
  - *Incident handling and mitigation strategies.*
  - *Computer forensic analysis for investigating security incidents.*
  - *Continuous security monitoring practices.*
  - *Understanding SOC operations and workflows.*
  - *Security data visualization for effective*

- *Adherence to cybersecurity policies and compliance.*
- *Integration of threat intelligence for proactive defense.*
- *Collaboration and communication with cybersecurity professionals.*
- *Continuous learning mindset in the dynamic cybersecurity field.*

- ***Application:***
  - *Actively contributed to the analysis of network traffic for threat detection.*
  - *Applied incident response strategies to mitigate security incidents.*
  - *Utilized computer forensic analysis for investigating security events.*
  - *Participated in SOC operations, including real*

Ethical Hacking and Network Monitoring

NTI | 08/2022

- ***Learned and Applied:***
  - *Comprehensive understanding of ethical hacking techniques.*
  - *Foot-Printing, Reconnaissance, and Vulnerability Analysis.*
  - *System hacking techniques and procedures.*
  - *Sniffing, Social Engineering, DDoS, and Session Hijacking.*
  - *Use of network monitoring tools to identify attacks against protocols and services.*
  - *Methods to prevent malicious access to networks, hosts, and data.*
  - *Investigation of endpoint vulnerabilities and attacks.*
  - *Evaluation of network security alerts.*
  - *Analysis of network intrusion data to identify compromised and vulnerable hosts.*
- ***Developed Skills:***
  - *Proficient in ethical hacking techniques.*
  - *Expertise in identifying and mitigating network vulnerabilities.*
  - *Skilled in analyzing and responding to network security alerts.*
  - *Competent in preventing malicious access to networks and data.*
- ***Application:***
  - *Applied ethical hacking methodologies for comprehensive network security.*
  - *Utilized network monitoring tools to identify and counteract attacks.*
  - *Investigated and mitigated endpoint vulnerabilities and attacks.*

CCNA

NTI | 07/2022

- ***Learned and Applied:***
  - *Network topology implementation.*
  - *Configuration of Cisco routers and switches.*
  - *Setup and management of VLANs and Layer 2 protocols.*
  - *Configuration of routing protocols, particularly OSPF.*
  - *Implementation of IP services, management, and monitoring protocols.*
  - *Securing network devices through techniques like Port Security.*
  - *Troubleshooting network issues for prompt issue resolution.*
- ***Developed Skills:***
  - *Expertise in configuring routers, switches, and network devices.*
  - *Proficiency in routing and switching.*
  - *Implementation of network security measures.*
  - *Troubleshooting network issues.*
  - *Network management skills.*
  - *Hands-on experience with Cisco networking equipment.*
- ***Application:***
  - *Actively involved in the implementation and configuration of Cisco networking equipment.*

- *Contributed to the establishment of efficient network communication.*
- *Applied security measures to ensure the integrity of network devices.*
- *Successfully resolved network issues through systematic troubleshooting.*

Technical Skills:

- ***Networking:***
  - *Configuration and administration of Cisco routers and switches.*
  - *Routing and switching protocols, including OSPF.*
  - *Deployment and management of VLANs and Layer 2 protocols.*
  - *Implementation of IP services, management, and monitoring protocols.*
  - *SSL-VPN configuration and troubleshooting.*
  - *Troubleshooting network issues.*
- ***Security:***
  - *Ethical hacking techniques, including Foot-Printing and Vulnerability Analysis.*
  - *System hacking, Sniffing procedures, DDoS, and Session Hijacking.*
  - *Network security implementation, including firewalls (FortiGate, Palo-Alto, Cisco ASA) and intrusion prevention systems.*
  - *Configuration of secure Virtual Private Networks (VPNs) - site-to-site and SSL.*
  - *Security policy deployment and management.*
  - *Endpoint vulnerability investigation and mitigation.*
  - *Log analysis and reporting using Forti-Analyzer.*
- ***Fortinet Technologies:***
  - *Deployment and administration of Forti-Manager 7.0.*
  - *Configuration and maintenance of Fortinet's FortiGate security appliances.*
  - *Security policy implementation for threat management and application control.*
  - *Deployment of VPN solutions on FortiGate devices.*
  - *Troubleshooting and issue resolution related to FortiGate devices.*
  - *Log analysis and reporting using Forti-Analyzer.*

Soft Skills:

- ***Communication:*** *Clear articulation of technical concepts to non-technical stakeholders.*
- ***Problem-Solving:*** *Proactive approach, root cause analysis, adaptability to challenges.*
- ***Leadership:*** *Team guidance, mentoring, and initiative-taking.*
- ***Time Management:*** *Prioritization, multitasking, meeting deadlines.*
- ***Teamwork and Collaboration:*** *Effective collaboration with cross-functional teams.*
- ***Adaptability:*** *Embracing change and flexibility in new environments.*
- ***Attention to Detail:*** *Meticulous in technical configurations and documentation.*
- ***Conflict Resolution:*** *Diplomacy and tact in addressing disagreements.*
- ***Organizational Skills:*** *Efficient task organization and documentation.*
- ***Continuous Learning:*** *Commitment to staying updated on industry trends.*

Certificates:

- ***Certified Ethical Hacker (CEH)***
  - *Certification Number: ECC7126593480*
  - *Certification link: elesawi.com/url/CEH*
- ***Fortinet FortiManager 7.0 Administrator***
  - *Certification link: elesawi.com/url/FMG*
- ***Fortinet Enterprise Firewall 7.0 Administrator***
  - *Certification link: elesawi.com/url/EFA*

Languages:

- ***Arabic:*** *Native*
- ***English:*** *Very Good*

References:

References are available upon request.