







PERSONAL INFORMATION Mostafa Elnakeb

 Stockholm, Sweden
 +46-(0)702772214
 mostafa.elnakeb@gmail.com
 <https://github.com/mostafaelnakeb/>
 <https://mostafaelnakeb.github.io/>
 <https://medium.com/@mostafa.elnakeb>

Sex Male | Date of birth 14/02/1992 | Nationality Egyptian

WORK EXPERIENCE

01/09/2022–Present

Senior DevSecOps (Leading Authority)| Security

Viaplay Group AB, Stockholm (Sweden)

Developed and implemented a comprehensive DevSecOps framework, integrating security practices into CI/CD pipelines and enabling security to shift left.

Led penetration testing efforts to identify vulnerabilities and mitigate risks, ensuring the resilience of critical systems and applications.

Oversaw risk management activities, conducting risk assessments, identifying threats, and implementing appropriate controls to protect organizational assets.

Implemented asset management processes to track and secure sensitive data, reducing the risk of data breaches and ensuring compliance with industry regulations.

Orchestrated vulnerability management programs, leveraging automated tools and processes to continuously monitor, assess, and remediate vulnerabilities across the organization's infrastructure.

Fostered a security shift left culture by championing secure coding practices, conducting security training sessions, and providing developers with the necessary tools and resources to proactively address security concerns.

Implemented security measures in CI/CD pipelines, including SAST and DAST, to detect and remediate vulnerabilities early in the software development lifecycle.

Developed applications using Python and GoLang, applying secure coding practices and adhering to industry standards.

Ensured AWS security by implementing best practices, conducting security audits, and securing cloud-based applications and infrastructure.

Implemented observability practices using Prometheus and Splunk, enabling comprehensive monitoring, alerting, and log analysis for enhanced system visibility and incident response.

01/03/2022–30/05/2022

Cyber Security Consultant

Conducted comprehensive vulnerability assessments for client systems and networks, identifying security weaknesses and recommending remediation measures.

Collaborated with clients to develop and implement vulnerability management programs, including vulnerability scanning, analysis, and

remediation.

Advised clients on best practices for building secure DevSecOps processes, integrating security into the software development lifecycle, and implementing secure coding practices.

Conducted architecture and security reviews of AWS environments to ensure adherence to AWS security best practices and industry standards.

Developed and implemented security controls, including IAM policies, VPC configurations, and security group rules, to safeguard AWS infrastructure.

Assisted clients in establishing incident response procedures, conducting security incident investigations, and implementing incident response plans.

Provided security guidance and recommendations to clients on compliance with relevant regulations, such as GDPR, HIPAA, or PCI DSS.

Delivered training sessions and workshops to educate clients' teams on cyber security best practices and awareness.

25/08/2019–07/02/2022

DevSecOps

Kambi AB, Stockholm (Sweden)

Configured and maintained Nessus vulnerability scanning tool to perform regular scans across the infrastructure.

Developed and implemented vulnerability scanning processes to identify security weaknesses and potential vulnerabilities within the systems.

Worked closely with AWS environments, implementing security best practices, and ensuring compliance with industry standards.

Collaborated with cross-functional teams to develop and implement effective remediation strategies for identified vulnerabilities.

Automated vulnerability scanning processes using scripting languages such as Python, and Bash.

Integrated vulnerability scanning tools with CI/CD pipelines such as SCA to enable continuous scanning and integration of security into the software development lifecycle.

01/04/2017–13/08/2021

Python Developer.

RedActive, Remote

Developed robust and secure Python-based security tools and APIs to facilitate log analysis, file analysis, and network traffic analysis.

Utilized Django and Flask frameworks to architect and implement scalable web applications and RESTful APIs for efficient data processing and analysis.

Collaborated closely with security teams to understand requirements and translate them into effective solutions that address their specific needs.

Applied data science techniques to extract valuable insights and patterns from large log datasets, enhancing threat detection and incident response capabilities.

Worked proficiently with diverse databases such as MySQL, MongoDB, and DynamoDB, ensuring efficient and reliable data storage and retrieval.

Employed GitLab for streamlined version control, enabling efficient collaboration and code management throughout the development process.

Leveraged Elasticsearch to efficiently index and search log data, facilitating advanced log analysis and search capabilities.

Utilized AWS services to ensure seamless deployment and scalability of applications, optimizing performance and resource utilization.

Utilized popular Python libraries, including NumPy, Pandas, and Matplotlib, to perform data manipulation, analysis, and visualization tasks effectively.

01/04/2017–13/08/2021

Cyber Security Consultant | Red Team Services

Secure Misr, Cairo (Egypt)

Perform thorough penetration tests on various systems, networks, and applications to identify vulnerabilities and potential security risks.

Conduct comprehensive vulnerability assessments to identify weaknesses in infrastructure, applications, and other digital assets.

Utilize ethical hacking techniques to exploit vulnerabilities and assess the impact on systems and data integrity.

Prepare detailed reports outlining findings, including vulnerability assessments, exploitation techniques used, and recommended remediation steps.

Stay updated with the latest security trends, emerging threats, and industry best practices to ensure effective penetration testing methodologies and techniques.

Assist in developing strategies and recommendations for mitigating identified risks, including implementing security controls and countermeasures.

Work closely with cross-functional teams, including IT and development teams, to ensure effective coordination and communication of penetration testing results and remediation efforts.

Ensure compliance with relevant industry standards, regulations, and frameworks such as PCI-DSS, ISO27K1, and GDPR.

Provide guidance and training to junior team members on penetration testing techniques, tools, and best practices.

Identify opportunities for process improvement and contribute to the development of new tools, methodologies, and techniques to enhance the effectiveness and efficiency of penetration testing activities.

Responded to customer questionnaires and audits, providing detailed information on security practices, policies, and processes, ensuring transparency, and meeting compliance obligations.

10/01/2016–30/03/2017

Security Operational Center (SOC) Analyst

Secure Misr, Cairo (Egypt)

Monitored network security events and alerts received from customer's monitored servers using various security monitoring tools.

Analyzed and investigated security incidents to identify potential threats and vulnerabilities.

Implemented SOC policies and procedures to ensure compliance and adherence to industry best practices.

Developed and refined rules and queries for ArchSight to enhance the detection of true positive security events.

Collaborated with cross-functional teams to investigate and respond to security incidents promptly.

Conducted thorough analysis of security alerts and incidents, determining their severity and potential impact.

Mitigated security incidents by taking appropriate actions based on established incident response procedures.

Conducted incident response activities, including containment, eradication, and recovery efforts.

Documented and reported security incidents, ensuring accurate and timely reporting to stakeholders.

Participated in incident post-mortem reviews to identify areas for

improvement and enhance future incident response processes.

16/12/2014–04/01/2016

DevOps Engineer

Arrow Technology , Cairo (Egypt)

Leveraged AWS services such as EC2, RDS, and S3 to enhance system scalability, reliability, and data storage.

Managed websites for the production system, including app.siliconexpert.com, on AWS to ensure availability and optimal performance.

Implemented and managed CI/CD pipelines using Jenkins, enabling continuous integration, testing, and deployment processes.

Managed Git repositories, ensuring proper version control and collaboration among development teams.

Developed Python, PowerShell, and Bash scripts to automate repetitive tasks, improving efficiency and reducing manual effort.

Monitored and fine-tuned JVM performance hosted on Oracle WebLogic and Apache Tomcat, utilizing various monitoring and profiling tools.

Administered high availability online Java-based systems on AWS, ensuring their smooth operation and optimal performance.

Built and maintained Solr indices to facilitate efficient search capabilities within the systems.

Configured Apache web server and Nagios monitoring system to ensure reliability and timely detection of issues.

Collaborated closely with the development and QA teams to streamline the software development lifecycle and ensure efficient delivery of applications.

EDUCATION AND TRAINING

01/01/2009–01/01/2014

BSc in Computer Science

EQF level 5

Faculty of Science - Cairo
University, Cairo (Egypt)

PERSONAL SKILLS

Mother tongue(s) Arabic

Foreign language(s)	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	B2	B2	B1	B2	B2

Communication	Having a good interpersonal and communication skills to share knowledge and to communicate effectively with different backgrounds.
---------------	--

skills	Having strong oral and written communication, organization, and interpersonal skills. Ability to translate complex findings into interpretable and simple output.
Organizational/managerial skills	Developing Business Strategy and providing Technical Thought leadership; Managing customer engagements escalations to ensure customer satisfaction; Expert understanding of technology and security principles and possessing knowledge of the cyber threat landscape; Expert in leading penetration testing and vulnerability assessment engagements for large enterprise firms.
Job-related skills	<p>Expert in tailored reconnaissance, exploitation, and lateral movement. Strong knowledge of attack surfaces for common enterprise systems and services.</p> <p>Be able to independently apply testing methods against a wide variety of targets including Web Applications, Mobile Applications, Web APIs, databases, wireless networks, conducting social engineering attacks against customer user base, routing infrastructure, VOIP, and VPN.</p> <p>Perform secure code review. Writing fully functional exploits for common vulnerabilities such as simple stack overflow, cross-site scripting, or SQL injection.</p> <p>Strong knowledge in scripting. Good experience with SIEMs (Splunk, ArcSight)</p> <p>Excellent experience with AWS. Writing security tools (Golang, Python, Java, and PHP)</p>

ADDITIONAL INFORMATION

Certifications

Offensive Security Certified Professional (OSCP)
 Certified Red Team Professional (CRTP)