IVAN GLINKIN
mail@ivanglinkin.com | www.ivanglinkin.com | www.linkedin.com/in/ivanglinkin
+971 58 5963066 | Dubai, United Arab Emirates

INFORMATION / CYBER SECURITY EXPERT

SUMMARY
Over **10 years** of experience working in cyber security including **penetration testing** of enterprise networks and web application, **establishing** information security programs and **ensuring** the **CIA** as well as **managing** mature information **security policies**, **governance**, **awareness**, vulnerability and risk **assessment** and **remediation**.

As an active member of the **Cyber Security** community, I have proven my skills in ethical hacking by identifying and responsibly disclosing security bugs: **remote code execution** on Stanford, HackTheBox, New York University and Martinos Center for Biomedical Imaging (Massachusetts General Hospital), **web admin** on Cambridge and MIT universities; McAfee **antivirus bypass**.

Knowledge of **Bash** Scripting, **PHP**, **SQL**, **Python** and **C-based** program languages allows me to create my own applications for automation and optimization company's security. **Close-Circuit Telegram vision**, **Fast Google Dorks Scan**, **AutoSUID** and **Domain checker** are some of my applications, which are widely recognized by big vendors like **Trend Micro**, **Deloitte**, **Splunk**, **Hakin9** and **KitPloit**.

In addition to my bug bounty and application development skills, I stay up to date with the latest industry standards and best practices by continuously pursuing professional education and certification. I hold several certifications such as the Certified Chief Information Security Officer (**CCISO**), EC-Council Information Security Manager (**EISM**), Certified in Cybersecurity (**CC**), Offensive Security Certified Professional (**OSCP**), **Certified Ethical Hacker** (Master), and Certified Network Defense Architect (**CNDA**).

As an information security expert, my goal is to improve security by **identifying** vulnerabilities and **implementing** effective solutions.

PROFESSIONAL EXPERIENCE
Deloitte
Senior Manager (Cyber Risk Advisory), October 2021 – till now
- Cooperated with the company's key account clients across the Globe leaded to sign contracts for penetration test and information security audit with global companies from the United States, Germany, Japan, Kazakhstan, and other
- Managed projects and developed cross-counties interconnections with cooperation with Deloitte Global Red Team from North America, Europe, and the Middle East
- Performed clients' penetration tests and found an unintended way to evade antivirus protection which led to harvesting critical confidential data and getting complete control over the domain
- Oversaw, leaded, mentored and taught subordinates who were able to pass one of the most complicated and demanding cybersecurity exams - OSCP
- Developed tools to aid penetration test automation and effectiveness such as **AutoSUID**, **ShellDAVpass** and **Domain_checker**

MegaFon
Cyber Security Analysis Expert, December 2020 – October 2021 (remotely)
- Created development plans for the customer's infrastructures, oversee its implementation and support it with automation and efficiency tools of his own
- Figured out all potential vulnerabilities in MegaFon client's infrastructure, systems, software, and operations
- Developed mitigation plans to counteract or eliminate cyber security risks before any actual incidents
- Created educational plans and events to raise security awareness among the client's employees

DataMe (AGGA Empire)
Information Security Manager, June 2017 – October 2021
- Cooperated with key account clients like Deloitte, Unilever, Valio, Miro, Heinemann, IFF Frutarom
- Developed tools to aid penetration test automation and effectiveness such as **Fast-Google-Dork-Scan**, CA "Hydra", Host- and Port Enumeration
- Performed internal and external pentest, web application testing (OWASP Top 10), and full-scope red teams
- Created threat models that result in more secure application design
- Wrote comprehensive and accurate reports, test plan documents, and mitigation recommendations

JSC Transneft
Lead Information Security Analyst, December 2014 – July 2017
Senior Information Security Analyst, July 2013 – December 2014
- Coached and managed a team of company's security up to 12 people
- Tested the company's information systems for penetration using BackTrack and Kali Linux applications like NMap, WFuzz, John the Ripper, SQLMap, Metasploit, Burpsuite, Wireshark, etc.
- Recognized and safely utilized attacker tools, tactics, and procedures
- Developed and implemented policies and procedures throughout the life cycle of the automatic leak detection system which prevented of unauthorized user's actions
- Develop policies, procedures and contingency plans to minimize the effects of security breaches from client's staff and criminals

EDUCATION
- **The Russian Presidential Academy of National Economy and Public Administration**
  ECE and WES approved as Master's degree | IT Management for Business, 2015 – 2018
- **Military University of the Ministry of Defense**
  ECE and WES approved as Master's degree | Jurisprudence, 2004 – 2009

CERTIFICATIONS
- Certified Chief Information Security Officer (CCISO), 2022-2024
- EC-Council Information Security Manager (EISM), 2022-2025
- Certified in Cybersecurity (CC), 2023-2026
- Offensive Security Certified Professional (OSCP), 2021
- Certified Ethical Hacker (Master), 2020-2026
- Certified Network Defense Architect (CNDA), 2020-2026
- Certified Network Defender (CND), 2020-2026

CVE
- **CVE-2024-24312 –** SQL injection (SQLi)
- **CVE-2024-24313 –** Insecure direct object references (IDOR)
- **CVE-2024-36821** – Security misconfiguration

PUBLICATIONS
- **Unveiling vulnerabilities in cybersecurity: A penetration test journey** – Deloitte ME, 04.2024
  https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/sustainable-strategies/unveiling-vulnerabilities-in-cybersecurity.html
- **AutoSUID** – Splunk (Approaching Linux Post-Exploitation with Splunk Attack Range), 01.2022
  https://www.splunk.com/en_us/blog/security/approaching-linux-post-exploitation-with-splunk-attack-range.html
- **The Russian Kerbrute** - Hakin9 (IT Security Magazine), 11,2021
  https://hakin9.org/the-russian-kerbrute-by-ivan-glinkin/
- **Data leaks without hacking** - Hakin9 (IT Security Magazine), 02.2021
  https://hakin9.org/data-leaks-without-hacking/
- **Fast Google Dork Scan** – KitPloit (PenTest Tools for your Security Arsenal), 06.2020
  https://www.kitploit.com/2020/06/fast-google-dorks-scan-fast-google.html