ANDI FITRA FURQAN

081244884454 | fitrafurqan@gmail.com | https://github.com/andiafif | linkedin.com/in/andi-fitra-furqan

Jl. Penerangan, Jelambar, Kec. Grogol petamburan, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta

Career as a Level 1 SOC Analyst, has progressed to an intermediate proficiency level in 1 year, with hands-on experience in triage, investigation, and mitigation of complex security incidents. Master the configuration and utilization of key devices such as **IBM QRadar, Cybereason, SIEM, XDR, and NDR** to protect data and systems. Utilizing *foundations* in the field of Informatics Engineering and *web development* for a more comprehensive *root cause* analysis , especially on *web-based vulnerabilities*.

Education

Fajar University - **Makassar, Indonesia** Sep 2018 - May 2023

- *Bachelor of Engineering-Department of Electrical Informatics Concentration, 3.32/4.00*
- Develop a deep understanding of various programming languages, including JavaScript, C++, and PHP and acquire skills in the analysis, design, and implementation of
- effective software solutions.
- Focus on web development, involving practical practice in designing, building, and managing responsive and interactive websites.
- Understand the basic principles of user interface (UI) and user experience (UX) design to create an engaging and easy web experience
- digunakan.
- Undertake an internship to gain practical insight into web development, working under the guidance of experienced professionals.
- Working on freelance projects in web development, which allowed me to apply my knowledge and skills independently and collaborate with various clients.
- Skilled in debugging and troubleshooting, as well as having a solid understanding of best software development practices.
- Familiarize yourself with continuous development (CI/CD) practices and integration with tools like Git.
- Skilled in designing and managing databases, as well as using SQL language to access data
- Possess basic cybersecurity analysis skills to identify potential risks and implement appropriate safeguarding measures.

Work Experience

PT. Kalla Group - **Makassar, Indonesia** Nov 2021 - Dec 2021

Internship

- Updating framawork, thereby improving system reliability and performance.
- Identify customer needs and integrate the inbound and outbound mail validation feature on PT. Kalla Group, which allows users to verify incoming and outgoing mail quickly and efficiently.
- Apply strict data validation techniques to ensure the accuracy and security of mail information stored in the system.
- Conduct thorough testing and debugging to ensure the quality and reliability of the mail validation feature.
- Ensure compliance with applicable data security and privacy standards in the development and storage of mailing information.
- Perform periodic maintenance, updates, and bug fixes on mail validation systems to maintain system performance and reliability over time.

PT. Neotech Horizon Indonesia - **West Jakarta,Indonesia** May 2025 – October 2025

Contract

- Monitor and analyze network and system activity using security monitoring tools (SIEMs)
- Identify potential threats or suspicious security events, such as unauthorized login attempts or strange activity on the network.
- Handle and respond to events that require immediate attention
- Respond to initial security incidents, such as malware attacks, DDoS, or data breaches.
- Identify and classify incidents based on their level of urgency and impact.
- Escalate to SOC Analyst Level 2 (L2) if needed.
- Conduct an initial analysis of detected incidents to determine whether they are a real threat or a false positive.
- Collect evidence and information related to incidents, such as logs, user activity, or infected files.
- Analyze and filter logs from various sources such as firewalls, servers, and network devices.
- Record and document incidents and findings for future reference.
- Compile an incident report detailing the analysis that has been carried out and the steps taken.

PT. Hipernet Indodata (HYPERNET) – **Central Jakarta, Indonesia** May 2025 – October 2025

Contract

- Monitor and analyze network and system activity using security monitoring tools (SIEMs)
- Identify potential threats or suspicious security events, such as unauthorized login attempts or strange activity on the network.
- Handle and respond to events that require immediate attention
- Respond to initial security incidents, such as malware attacks, DDoS, or data breaches.
- Identify and classify incidents based on their level of urgency and impact.
- Escalate to SOC Analyst Level 2 (L2) if needed.
- Conduct an initial analysis of detected incidents to determine whether they are a real threat or a false positive.
- Collect evidence and information related to incidents, such as logs, user activity, or infected files.
- Analyze and filter logs from various sources such as firewalls, servers, and network devices.
- Record and document incidents and findings for future reference.
- Compile an incident report detailing the analysis that has been carried out and the steps taken.

Other Skills and Experience

- **Modules Taken (**2025): Certified Incident Handler (ECIH) di Ec Council
- **Modules Taken (**2025): Certified Incident Handler (ECIH) di CouseNet Indonesia
- **Modules Taken (**2024): Certified Ethical Hacker (CEH) di Ec Council
- **Modules Taken (**2024): Certified Ethical Hacker (CEH) di CourseNet Indonesia
- **Modules Taken (**2024): ComTIA Security+ (SY0-701) Complete Course & Exam di Udemy
- **Modules Taken** (2023): Ethical Hacking V3 di Xcode.com
- **Modules Taken** (2022): Belajar Dasar Pemrograman JavaScript di Dicoding.com
- **Modules Taken** (2022): Cloud Practitioner Essentitals (Belejar Dasar AWS Cloud) di Dicoding.com
- **Soft Skills**: Problem Solving, Critical Thinking, Manajemen Waktu, Kemampuan Komunikasi, Kerjasama Tim,
- **Hard Skill :** PHP(Intermediate), Framework Laravel 6 dan 7(Intermediate), CI 3(Intermediate), Microsoft Office(Intermediate), CSS(Beginner), JavaScript(Beginner), C++(Beginner), Networking(Beginner), Pentesting(Beginner), Maintenance Server(Beginner), Linux Administrator (Intermediate), SqlInjection(Intermediate), Nosql(Beginner),BurpSuite(Beginner),LFI(Beginner),RCE(Beginner),Cryptograph(Beginner),AnalisisWalware(Intermediate),DoS(Intermediate), Hacking(Intermediate), Vulnerability Assessment(Beginner),Firewall(Beginner),Digital Forensic(Beginner),Qradar(beginner), Azure Sentinel (Beginner), Rapid7 (Beginner)