IRFAN FITRI

Bin Mohd Sani

SENIOR CYBERSECURITY ANALYST

SOC OPERATIONS & THREAT INTERLLIGENCE

CONTACT

+6014-3509234 （Whatsapp）
Irfanfitri.work@gmail.com
Linkedin.com/in/irfanfitri

KEY SKILLS

Core Security Domains

- SOC Operations & Incident Response
- Threat Hunting & Detection Engineering
- Email Security & Anti-Phishing
- Endpoint Detection & Response (EDR/XDR)
- Firewall & Network Security
- Vulnerability Management & Penetration Testing
- Security Awareness & Phishing Simulation

Tools & Platforms

- CrowdStrike Falcon (EDR, NG-SIEM, Threat Hunting)
- FortiGate Firewall
- TrendMicro Email Security
- Cloudflare (WAF, CDN)
- Delinea Secret Server (PAM)

Scripting & Automation

- Linux / Bash automation
- Log analysis
- Custom Detection Workflow

ABOUT ME

Senior Cybersecurity Analyst with hands-on experience leading SOC operations, endpoint detection, email security, and firewall management in a large enterprise environment.

Specialized in threat hunting, phishing investigation, spoofing detection, incident response, and security automation using CrowdStrike Falcon, FortiGate, Trend Micro, and Linux scripting.

Proven track record in protecting large-scale user environments, strengthening detection capabilities, and driving organization-wide security awareness programs.

EXPERIENCE

SENIOR CYBERSECURITY ANALYST

IMU UNIVERSITY

KUALA LUMPUR, MALAYSIA

OCTOBER 2024 – PRESENT

Lead end-to-end cybersecurity operations to protect the university's digital environment and maintain compliance.

Key Responsibilities:

- Lead SOC operations protecting university environment covering thousands of users and endpoints across academic and clinical systems.
- Perform proactive threat hunting using CrowdStrike Falcon EDR and Next-Gen SIEM to detect suspicious activity and reduce incident response time.
- Administer Microsoft Defender for Endpoint and Microsoft Defender for Office 365, investigating endpoint and email-based security incidents.
- Manage Trend Micro Email Security, handling phishing investigations, spoofing detection, quarantine workflows, and user incident reports.

Language

- English (Native Speaker)
- Mandarin (Native Speaker)
- Bahasa Malaysia (Native Speaker)

EDUCATION

BSC (HONS) IN COMPUTER SCIENCE (CYBER SECURITY)

ASIA PACIFIC UNIVERSITY & INNOVATION (APU)

2021 – 2023

DIPLOMA IN INFORMATION SYSTEM ENGINEERING

TUNKU ABDUL RAHMAN UNIVERSITY COLLEGE (TARUC)

2017 – 2020

- Design and execute organization-wide phishing simulation campaigns using Microsoft Attack Simulation Training, improving user awareness and reducing phishing click-through rates.
- Develop and deliver cybersecurity awareness training modules to strengthen staff security posture against social engineering threats.
- Administer FortiGate firewalls including SSL inspection, IPS policies, VPN and external dynamic blocklists (EDL) to strengthen perimeter defense.
- Automate SOC workflows using CrowdStrike Falcon Workflow to run detection logic and remediation actions, improving response efficiency and detection consistency.

SECURITY ENGINEER

DIGITAL DEFENSE SOLUTION SDN BHD

KUALA LUMPUR, MALAYSIA

JUNE 2024 – AUGUST 2024

- Deploy and maintain Privileged Access Management (PAM) solutions using Delinea Secret Server to secure privileged credentials and access workflows.
- Implement and manage Content Delivery Network (CDN) and security services using Cloudflare, improving application performance and web security posture.
- Troubleshoot advanced security solutions and resolve technical issues to ensure system stability and optimal protection.
- Provide technical support and security expertise to enterprise clients, ensuring robust security controls and service reliability.
- Collaborate with cross-functional teams to design, implement, and deliver comprehensive security solutions for customer environments.
- Stay current with emerging security threats, technologies, and best practices to enhance service offerings and solution effectiveness.

TECHNICAL SUPPORT ENGINEER (CYBER SECURITY)

EDGENEXT

KUALA LUMPUR, MALAYSIA

JANUARY 2023 – MAY 2024

- Monitor, detect, and mitigate Distributed Denial-of-Service (DDoS) and Challenge Collapsar (CC) attacks to protect customer web services and online platforms.
- Perform real-time traffic analysis and apply mitigation strategies to ensure uninterrupted availability of client websites and applications.
- Respond rapidly to security incidents and customer escalations, minimizing service disruption and business impact.
- Communicate directly with global clients to investigate security issues, provide status updates, and deliver timely resolutions.
- Coordinate with internal engineering teams to fine-tune defense policies and improve attack detection accuracy.
- Support a global customer base across multiple time zones, demonstrating flexibility and effective technical communication.

SOLUTION AND DELIVERY (INTERNSHIP)

ITGROUP, INC (PHILIPPINES)

KUALA LUMPUR, MALAYSIA

JANUARY 2022 – APRIL 2022 (16 WEEKS)

- Provide staff support and assist in managing client data within Oracle NetSuite enterprise systems.
- Participate in daily cross-border virtual meetings with teams in the Philippines, Singapore, and Malaysia to coordinate task updates and delivery progress.
- Support solution delivery activities including system configuration, testing, and documentation.
- Assist in tracking project tasks and ensuring timely completion of assigned deliverables.

JUNIOR DEVELOPER

WHITELABLE STARTUP (SABAH)

KOTA KINABALU, MALAYSIA

FEBRUARY 2019 – NOVEMBER 2020

- Design and develop front-end websites and mobile applications for client projects using modern web frameworks.
- Build responsive user interfaces using MaterializeCSS and Bootstrap to ensure cross-platform compatibility and usability.
- Collaborate with designers and backend developers to deliver functional and visually consistent applications.
- Perform testing, debugging, and enhancement of existing web and mobile applications.