Michael Cahyadi

+6285810871612 | hi@meekolab.com | research.meekolab.com | maikxchd | Michael Cahyadi

Skills

Platform	Amazon Web Services • Google Cloud Platform • Microsoft Azure • VmWare vCenter/ESXi
Security (Endpoint)	CyberArk PAM • Cybereason XDR • Crowdstrike Falcon • Jumpcloud SSO • Checkpoint Harmony • Forcepoint ONE
Security (Network)	Fortinet FortiGate • Forcepoint SWG • Forcepoint ZTNA • Ivanti Connect Secure • Tenable One
Security (Forensics)	Cellebrite Physical Analyzer • OpenText Encase Forensic • Nextron THOR • Cerbero Suite
Security (Cloud)	Terraform • PagerDuty • Sonarcloud • Datadog • DEVO SIEM/SOAR

Work Experience

Traveloka — Banten, Indonesia

Traveloka is one of the biggest Online Travel (OTA) and events platform in Southeast Asia, with more than 42 million monthly active users

Security Engineer, Security Operations — **June 2023 - Present**

- Became one of the Proof-of-Concept implementators for the Forcepoint Secure Service Edge (SSE) project, which includes Zero Trust Network Access (ZTNA), Data-Loss Prevention (DLP), and Cloud Access Security Broker (CASB) tools, worked on the Usability testing and Detection capabilities of Forcepoint Neo DLP Agent, resulting in a 34% performance boost on endpoints compared to previous DLP agent solutions
- Performed security audits adhering to standards such as PCI DSS, ISO 27001, and SWIFT CSP, with a focus on enhancing security monitoring, logging architecture, and incident response strategies
- Worked alongside the Site Reliability Engineering (SRE) teams in resolving two DDoS incidents and scraper bots, with the implementation of AWS WAF Shield Advanced and AWS Bot Control leading to a 73% reduction in both activity without any reported false positives
- Led consultation efforts across different tech teams for the reduction of vulnerabilities in 180+ AWS accounts by 30% per month for one quarter using AWS Inspector alongside internally developed tools, totalling to patching more than 1.6 million common vulnerabilities
- Participated in the detection, recovery, and forensics of a major security breach incident which required an emergency VPN migration within 48 hours, resulting in the switch of 2000 users to a new VPN infrastructure with only 30 minutes downtime
- Conducted 400+ security incident triages, including two major zero day incidents, using Cybereason XDR for malware detection, DEVO SIEM for alert analysis, along with forensic evaluations on Windows and macOS systems and achieved 44% reduction in MTTR
- Conducted an Attack Detection Capability Assessment (ADCA) exercise alongside WithSecure, and used the information to work with technical and support teams from Cybereason to identify and patch more than 126 detection lapses with the XDR and MDR product

Finku (YC W22) — DKI Jakarta, Indonesia

Finku is a YCombinator-backed fintech company offering Personal Finance Management (PFM) services with more than 600,000 users

Cloud Infrastructure Consultant — **October 2022 - November 2023**

- Managed a secure, multi-cloud infrastructure in compliance with OJK regulations, using AWS ECS, Google Kubernetes Engine, and BigQuery
- Engineered and deployed AWS WAF Shield, achieving a 93% reduction in API-targeted web attacks, enhancing overall cybersecurity posture
- Built a scraping system to retrieve and aggregate financial data from multiple banks using Selenium, Puppeteer, OpenSTF/DeviceFarmer
- Merged the operation of several Machine Learning workloads in Google Kubernetes Engine (GKE) and was able to achieve a 56% reduction in operational costs without any impact to performance and accuracy
- Designed the architecture of a secure cloud environment for a Virtual Card Number service with a major local bank, leveraging technologies like Redis, Kafka, and AWS ECS, focusing on scalability and security

Sayurbox — DKI Jakarta, Indonesia

Sayurbox is a leading Indonesian e-grocery platform that connects around 10,000 farmers with more than 400,000 active users per month

DevSecOps Engineer — **March 2022 - August 2022**

- Conducted in-depth security investigations and remediation of over 300 vulnerabilities within GCP and AWS environments, leveraging threat intelligence from local security vendors and implementation of security best practices
- Validated more than 60 exploits in liaison with a third-party cybersecurity firm to appropriately hand out bounty payments accounting for the severity of the vulnerability and the priorities of the firm
- Designed and implemented cloud-native security solutions in line with SOC 2 and ISO 27001 standards, using AWS EKS, Jenkins, Ansible, and Istio Service Mesh
- Orchestrated vulnerability monitoring and Cloud Security Posture Management using Deepfence Threatmapper, enhancing security visibility and compliance
- Created a method to reduce Datadog logging spending by migrating cold storage logs older than 1 month into S3 buckets, utilizing S3 One Zone Infrequent Access and saving $11,122 per month in cloud operations cost
- Conducted security investigations and remediation of vulnerabilities within a microservices architecture and managed security incident responses for compromised executive Google Workspace accounts

Projects

Meekolabs (research.meekolab.com) — Indonesia

Independent Security Research — 2021 - Current

- Authored a blog called Meekolabs, which provides a range of articles and in-depth research on EDR bypass, network red teaming, Windows and Mac forensic techniques, and other niche security research
- **Acknowledgements**: Articles have been featured as citations in BSides Singapore 2023, Bsides London 2024, and CDEF Indonesia 22nd Meetup

What Is Up, Indonesia? (WIUI) — Indonesia

Independent Media Organization — 2022 - Current

- What Is Up, Indonesia is an independent media organization that curates socio-political issues in Indonesia, with cooperation with the EU Policy and Outreach Partnership Program, the UN High Commissioner for Refugees, and the US State Department
- Provided operational security consulting and remediation services, successfully fended off three cases of politically-motivated cyberattacks against the organization website and personal devices of organization members

Education

BINUS University — DKI Jakarta, Indonesia

Bachelors Degree in Computer Science, Cybersecurity — 2020 – 2024