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 • Jumpcloud MDM & SSO • Forcepoint ONE • Forcepoint Security Manager
Security (Network)	Fortinet FortiGate • Ivanti Connect Secure • Tenable One • Forcepoint Bitglass SSE
Security (EDR)	Cybereason XDR • Crowdstrike Falcon • SentinelOne • Cisco Secure Endpoint • TrendMicro Vision ONE
Security (Cloud/SaaS)	Terraform • Datadog • DEVO SIEM/SOAR • Checkpoint Harmony Email Gateway • Palo Alto Prisma Cloud

Work Experience

Superbank (a Grab Company) — Indonesia

Superbank is the banking subsidiary of Grab Holdings, an app for ride-hailing, payments, and food delivery with more than 38.5mn users

Infrastructure Security Specialist — **September 2024 - Present**

- Validated the infrastructure implementation for core banking platform functions such as Real Time transfers through Indonesia's National Clearing House (BIFAST) and integration with credit scoring systems (SLIK OJK)
- Became one of the Proof-of-Concept implementors for Forcepoint ONE, worked on testing the Usability and Detection capabilities of Forcepoint F1E DLP and Forcepoint BitGlass Agent, resulting in a 34% performance boost on endpoints compared to previous DLP agent solutions
- Built 10 different Golden Images for four different operating systems in accordance to STIG HIGH hardening guidelines for Windows, Ubuntu, RHEL, and CentOS

Traveloka — Singapore

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

Security Engineer, Security Operations — **June 2023 - September 2024**

- 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
- Collaborated with AWS to create an intelligent threat detection solution in ECS Fargate with AWS GuardDuty for ECS Fargate, which increased security visibility across +2500 containers
- Finetuned the detection rules for Checkpoint Harmony Email Gateway to achieve 99% success rate for protection against 156 different email phishing tests in an environment that received 7.61 million emails every 14 days
- 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 866 security incident triages 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

Finku (YC W22) — Indonesia

Finku was a YCombinator-backed fintech company offering Personal Finance Management (PFM) services with more than 600k 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 — Indonesia

Sayurbox is a leading Indonesian e-grocery platform that connects around 10k farmers with more than 400k 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
- 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

Projects

Meekolabs (research.meekolab.com) — Indonesia

Independent Security Research — 2021 - Current

- Authored a blog called Meekolabs (Engineering Deficiency), 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, CDEF Indonesia 22nd Meetup, and Fortra's Blogpost about Mac & Linux Security

Supreme Kernel Stack Destroyers (SKSD) — Indonesia

Capture The Flag Group — 2024 - Current

- Part of the SKSD Capture The Flag Group, which scored 9th place globally in CTFTime.org in 2023

Education

BINUS University — DKI Jakarta, Indonesia

Bachelors Degree in Computer Science, Cybersecurity — 2020 – 2024