TRI WIBOWO CAHYO

Security Operations Center Analyst | Purple Team Specialist

"Purple Team specialist combining offensive security expertise (Top 5 Indonesia TryHackMe, 500+ day streak) with defensive operations experience in enterprise SOC environments. Proven ability to bridge red and blue teams through threat hunting, SIEM engineering, incident response, and adversary simulation. 3+ years technical experience spanning security operations, penetration testing, and infrastructure support."

Malang, East Java, Indonesia 0823 2800 2098 twibowo288@gmail.com Tri Wibowo Cahyo

WORK EXPERIENCES

Security Analyst - PT Mitra Pinasthika Mulia (MPM Distributor)

october 2025 - Present | Hybrid

- **Monitor 10,000+ daily security events** using IBM QRadar SIEM with custom AQL queries, reducing false positives by 40% through fine-tuned correlation rules and automated threat detection
- **Orchestrate automated incident response** via TheHive SOAR platform with auto-ticket creation, multi-source threat intelligence enrichment, and automated IP blocking
- **Conduct proactive manual threat hunting** identifying sophisticated attacks including malicious user agents, LOLBin abuse, web application exploitation, and data exfiltration attempts
- **Investigate security incidents** across Palo Alto Cortex XDR, Microsoft Defender for Office 365, and NDR solutions, blocking 200+ phishing campaigns monthly through comprehensive email analysis
- **Develop AQL detection queries** for suspicious URL patterns, authentication anomalies, and file upload monitoring across enterprise infrastructure

Red Team Intern - Hack Secure

April 2025 - May 2025 | (Remote)

- **Executed comprehensive penetration testing operations** using industry-standard tools (Nmap, Burpsuite, SQLMap) to identify critical vulnerabilities across web applications and network infrastructure
- **Performed advanced adversary simulation exercises** utilizing Metasploit, Empire, and Starkiller C2 frameworks to simulate real-world attack scenarios and test organizational security posture
- **Conducted web application security assessments** including SQL injection, XSS exploitation, and directory enumeration attacks, successfully identifying and documenting security weaknesses
- **Delivered actionable security reports** documenting vulnerabilities, attack vectors, and remediation strategies based on comprehensive red team assessments and CTF challenge completions

L2 Support Engineer - PT Solusi247

April 2023 - April 2025 (2 Years) | Hybrid

- **Delivered critical L2 technical support for AI/ML platforms** by diagnosing complex backend infrastructure issues and implementing automated solutions using SQL, Bash, and Python scripting
- **Performed systematic root cause analysis and incident triage** to identify underlying system issues and implement preventive measures, developing analytical thinking essential for security assessments
- **Managed high-pressure incident escalations** within SLA requirements, developing operational resilience and real-world incident response capabilities essential for cybersecurity operations
- **Automated system troubleshooting workflows** using Python and Bash scripting, improving operational efficiency and reducing manual intervention in critical security infrastructure

CYBERSECURITY PROJECTS

GhostStager | Advanced C# Fileless Malware Loader

- Built fileless malware framework with reflective PE loading, AMSI/ETW evasion, and Sliver C2 integration for red team operations
- Purple Team Value: Documented evasion techniques to improve defensive monitoring and endpoint detection capabilities

Astaroth-Style Red Team Campaign | LOLBin Abuse Simulation

- Executed sophisticated fileless attack using LOLBins (mshta.exe) mimicking APT tactics
- Purple Team Value: Developed detection rules and hunting queries to identify LOLBin abuse patterns in enterprise environments

Internal Pentest: Active Directory Exploitation

- Comprehensive AD penetration testing demonstrating Kerberoasting, AS-REP Roasting, privilege escalation, and lateral movement
- Documented exploitation paths and remediation strategies for AD misconfigurations

SIEM Detection Engineering | Threat Hunting Queries

- Developed custom AQL queries for IBM QRadar covering suspicious patterns, malicious user agents, and authentication anomalies
- Created correlation rules with **40% false positive reduction** through continuous tuning

25+ Hacktrace-Ranges CTF Writeups

- Detailed technical writeups demonstrating exploitation techniques across diverse attack vectors and operating systems
- **Top 20 ranking** on Hacktrace-Ranges platform

🔔 ***Portfolio:*** *cybersecurity compiled projects*

TECHNICAL SKILLS

Offensive Security	Burp Suite, SQLMap, Metasploit, BloodHound, Mimikatz, Impacket, CrackMapExec, VBA/C# Exploit Development, OWASP Top 10, Network Pivoting
Deffensive Security	IBM QRadar, Wazuh, Splunk, AQL, TheHive SOAR, Palo Alto Cortex XDR, Microsoft Defender, Cyber Threat Intelligence, NDR, Log Analysis, Detection Rules, Threat Hunting
Infrastructure & Platform Support	AWS (EC2, S3), Kubernetes, Apache Airflow DAG Management, Grafana, Apache Superset, MLCore, Dremio, Apache NiFi, Cloudera Flow Management, Hadoop Ecosystem, Spark-SQL, Dependency Tracing, Data Pipeline Troubleshooting, Python, Bash, SQL - Log Analysis, Sanity Testing, Whitelist Management

CERTIFICATIONS & RANKS

- **Certified API Security Practitioner** – APISEC University
- **Red Team Internship Certification** – HackSecure
- **Practical Ethical Hacking** – TCM Security
- **Practical Web Application and Testing** – TCM Security
- **Practical Web Hacking** – TCM Security
- **IT Support** - Google
- **TryHackMe Top 5 – Indonesia** (500+ day streak, 95.000+ points)
- **Hacktrace Ranges Top 20**

EDUCATIONS & CONTINOUS LEARNING

2025 - Present

Practical SOC Analyst Associate (PSAA) - TCM Security

The PSAA is an associate-level introduction to the world of security operations, covering areas such as phishing analysis, network traffic analysis, security monitoring, endpoint security, threat intelligence, SIEM, digital forensics, and incident response.

2012 - 2015

SMK Diponegoro Tumpang - Teknik Komputer Jaringan (TKJ)

・ IT Division Head at OSIS (Student Council) for 2 years: Led the IT division, overseeing school-wide tech initiatives, managing IT infrastructure, and collaborating with other departments to enhance digital experiences for students and staff

・ Internship at ITN Malang (Institut Teknologi Negeri Malang) as an IT Support Technician for 6 months: Provided technical support, troubleshooting, and maintenance for campus networks and systems, contributing to smooth operations and system enhancements