

CHRISTINA APRIANI

Batang, Indonesia | +62 822-1072-6180 | aprianichristina0@gmail.com

<https://www.linkedin.com/in/christina-apriani/> | <https://christinaapriani.netlify.app/> | <https://github.com/christina-apriani>

EXECUTIVE PROFILE

IT and cybersecurity professional with more than 12 years of experience in software development, network infrastructure, and security operations. Served as lead developer of an intelligence system for national law enforcement agencies. For the past two years, led enterprise network operations, the NOC, and data security at a National Strategic Project (PSN) industrial estate. Makes decisions on system resilience, fiber optic network expansion, cyber incident response, and CAPEX/OPEX budgets. Works hands-on with penetration testing, traffic analysis, digital forensics, and reverse engineering tools in CSIRT and SOC work, complemented by extensive executive experience managing cloud infrastructure, XDR ecosystems (including CrowdStrike and SentinelOne environments), and Zero Trust Architecture.

CORE COMPETENCIES

- **Infrastructure, Cloud & Hardware:** Enterprise Network Operations, Cloud Infrastructure Security, FTTH & GPON ecosystem (OLT, ODF, ODC, ODP, ONT), CCTV Command Center, Access Point Management, LAN/WAN, SCADA Integration.
- **Blue Team & Security Operations:** CSIRT Leadership, Zero Trust Architecture (ZTA), Enterprise Network Security Monitoring, Incident Triage & Severity Handling (SLA), SOC, SIEM, Wazuh, Palo Alto Cortex XDR, CrowdStrike, SentinelOne.
- **Red Team & Penetration Testing:** Vulnerability Assessment, Server Hardening. Cobalt Strike (APT simulations), BloodHound (Active Directory hacking), Maltego (OSINT), Kali Linux, Nmap, Nessus, Nikto, Burp Suite, Metasploit.
- **Purple Team, Forensics & Malware Analysis:** MITRE ATT&CK Framework, YARA rule writing, Volatility (RAM forensics), FTK Imager, The Sleuth Kit, Ghidra, IDA Pro, Cuckoo Sandbox.
- **IT Governance & Systems Development:** ISO/IEC 27001 (ISMS), ISO 9001 (QMS), ISO 14001 (EMS), Business Impact Analysis (BIA), Business Continuity Plan (BCP), Risk Management, BSSN Cybersecurity Maturity Index (IKAS). Microservices Security, Database Architecture, RabbitMQ, Redis Clustering, Agile SDLC, Secure Coding, Secure Code Review, Software Design Description (IEEE 1016-2009).

WORK EXPERIENCE

PT Kawasan Industri Terpadu Batang (KITB) | August 2024 - September 2026

Head of Operation Digitalization Department

- Led compliance with enterprise operating standards and took the company through integrated ISO/IEC 27001 (information security), ISO 9001 (quality management), and ISO 14001 (environmental management) certification. Completed the BSSN Cybersecurity Maturity Index (IKAS) assessment.
- Designed and enforced Zero Trust Architecture (ZTA) principles across the enterprise network to secure endpoints, hybrid cloud assets, and SCADA infrastructure.
- Managed physical IT infrastructure from planning to operation. Handled the fiber optic topology directly, from the central distribution point to customer endpoints: OLT configuration, ODF termination on the NOC side, route distribution through ODC and ODP, and ONT activation at tenant facilities.
- Built and ran the Network Operations Center (NOC) for enterprise network security monitoring. Kept system availability at 99.9% by combining data from the Wazuh-based SIEM, the SOC, SCADA sensors, hundreds of access points, LAN/WAN links, and the CCTV Command Center.
- Analyzed network traffic with Wireshark, tcpdump, and Zeek to trace suspicious connections across NOC and tenant segments. Used Splunk alongside Wazuh to correlate device and server logs during incident investigations, applying analytical frameworks highly compatible with Palo Alto Cortex

XDR. Led the corporate Computer Security Incident Response Team (CSIRT). Mapped cyber threats and infrastructure vulnerabilities using the MITRE ATT&CK Framework, then handled incidents by severity (Critical, High, Medium, Low) against strict mitigation SLAs.

- Authored custom YARA rules to proactively detect sophisticated malware signatures, acquired digital evidence with FTK Imager, and examined it with The Sleuth Kit to rebuild incident timelines.
- Prepared the annual IT budget (CAPEX and OPEX) using EFE Matrix, AHP, and BCG Matrix analysis. Cut internet service costs by up to 20% through vendor performance audits and ISP SLA renegotiation.

PT Astra Welab Digital Arta (AWDA) | June 2019 - July 2024

Senior Tech Development Division Head

- Led 18 technicians and engineers in building a secure-by-design microservices architecture for financial systems. Applied strict data encryption to protect the Personally Identifiable Information (PII) of millions of customers from leaks.
- Managed enterprise endpoint security and XDR environments for 5 years, utilizing advanced incident response methodologies and telemetry analysis fundamentally identical to CrowdStrike Falcon and SentinelOne.
- Protected cloud infrastructure and database integrity. Monitored Web Application Firewall (WAF) anomalies through Splunk dashboards and closed access gaps as soon as they appeared.
- Conducted deep memory and RAM forensics using Volatility to investigate advanced behavioral anomalies within the enterprise cloud infrastructure.
- Audited Active Directory (AD) privileges and mapped complex attack paths using BloodHound to eliminate lateral movement risks. Audited the strength of internal account password hashes with Hashcat and John the Ripper.
- Ran pre-release penetration tests on web applications and APIs with Kali Linux, Burp Suite, and Nikto. Used Metasploit to prove whether an attacker could actually exploit each finding before the team fixed it.
- Analyzed native libraries in mobile app builds and third-party SDKs with Ghidra to find hardcoded API keys and hidden functions before release.
- Set security standards for every phase of the Software Development Life Cycle (SDLC). Tracked system requirements with a Requirements Traceability Matrix so each feature release passed IT compliance audits by banking regulators.

PT FIRSTWAP INTERNATIONAL | December 2013 - April 2019

Senior Lead Software & Security Engineer

- Served as lead developer of the ALTAMIDES software ecosystem, an investigation and intelligence tracking system for national law enforcement agencies. Focused on encrypted data communication over closed networks.
- Deployed Cobalt Strike to conduct advanced persistent threat (APT) simulations and assess the real-world resilience of critical intelligence networks.
- Utilized Maltego to perform complex Open-Source Intelligence (OSINT) gathering and visualize link analysis for threat actor profiling.
- Designed a high-performance back-end with RabbitMQ and Redis Clustering. The back-end processed millions of telecom traffic records in real time.
- Hardened Linux CentOS servers. Closed unneeded open ports and reduced the risk of outside intrusion, including zero-day threats, on sensitive data assets. Verified each hardening round with Nmap scans and Metasploit exploit tests from Kali Linux.
- Led secure code reviews in the developer team to stop backdoors and exploitable flaws before the team deployed systems to law enforcement users. Analyzed compiled binaries and third-party libraries with IDA Pro.
- Tested suspicious files and attachments in Cuckoo Sandbox to observe malware behavior before the files reached the development environment.

Gramedia Bookstore | June 2012 - December 2013

IT Developer & Systems Administrator (Part-time)

- Built an internal logistics inventory application with Java and Oracle Database. Applied layered Role-Based Access Control (RBAC) to protect data integrity from internal tampering and database injection attacks.
- Maintained the store LAN and data sync to the head office server over WAN. Kept every Point of Sale (POS) terminal online, especially during peak transaction hours.

EDUCATION

Master of Technology Management (MMT) | Institut Teknologi Sepuluh Nopember (ITS) | Expected Graduation: Feb 2027

- **Thesis:** Evaluating Fiber Optic Infrastructure Service Security Quality and Tenant Satisfaction in an Industrial Estate Using SERVQUAL and PLS-SEM Modeling.

Bachelor of Information Systems (S.Kom) | Universitas Gunadarma | Graduated: Dec 2013

PROFESSIONAL CERTIFICATIONS & STANDARDS

- Certified Ethical Hacker (CEH) - EC-Council
- Certified Computer Forensics Analyst (CCFA) - eSecurity Institute & ABSD (Awarding Body for Sustainable Development)
- ISO/IEC 27001 Information Security Management System (ISMS) Implementer
- QRMO (Qualified Risk Management Officer) - BNSP