N.W. CHANAKA LASANTHA

Security Architect | Threat Detection & Response Leader | Post Doctoral Researcher | PhD | MSc | BIT | City & Guilds | MBCS | Cybersecurity GRC Strategist | Senior Lecturer

☎ +94-71-5807577
✉ chanaka.lasantha@gmail.com
○ Colombo, Sri Lanka
LinkedIn Profile

★ PROFESSIONAL SUMMARY

Results-driven Security Operations Manager with **25 years** in cybersecurity, specializing in Threat Detection & Response (TDR), SOC operations and delivery, and end-to-end incident management. Proven track record leading SOC teams, managing SIEM/EDR/NSM platforms (Microsoft Sentinel, Splunk, Wazuh), ensuring client SLA/KPI adherence across multi-client engagements. Expertise in MITRE ATT&CK frameworks, automated incident response, and Zero Trust architecture across AWS, Azure, and GCP. PhD researcher in AI-driven cybersecurity with 9+ peer-reviewed IEEE publications and active Senior Visiting Lecturer at multiple UK universities.

⚙ CORE COMPETENCIES

- **SIEM Platforms:** Microsoft Sentinel, Splunk, Wazuh, ELK
- **EDR/Endpoint:** CrowdStrike, Carbon Black, MS Defender
- **NSM/Network:** Darktrace, ExtraHop, Fidelis
- **SOC Operations:** TDR, Incident Mgmt, SLA/KPI, Threat Hunting
- **Frameworks:** MITRE ATT&CK, NIST, ISO 27001, PCI DSS, GDPR
- **Cloud & IoT/OT:** AWS, Azure, GCP, IoT Security
- **Scripting/Query:** Python, RegEx, SQL, Bash, Perl
- **Leadership:** SOC Team Mgmt, Client Engagement, DevSecOps

☰ TECHNICAL SKILL PROFICIENCY

SIEM (Sentinel/Splunk)
Incident Response
Cloud Security (AWS/Azure/GCP)
Python / ML Automation
SOC Operations & Delivery
EDR / Endpoint Security
Network Security Monitoring
GRC & Compliance

◆ PROFESSIONAL EXPERIENCE

KERNER NORLAND LTD | *Sri Lanka* — *Apr 2023 – Present*
Chief Security Architect & SOC Operations Lead

- **SOC Impact:** Decreased security incidents by 93% through SOC-driven ML/AI detection; reduced MTTR from 4 hours to 45 minutes via automated incident response workflows.
- **Compliance:** Achieved 100% compliance across ISO 27001, GDPR, PCI DSS, FedRAMP, NIST. Authored SOPs for SOC operations and GRC framework.
- **Architecture:** Implemented Zero Trust across multi-cloud (AWS, Azure, GCP). Built hybrid ML models for IP reputation validation with AWS WAF and GuardDuty.
- **Leadership:** Led security operations team across 5 locations. Delivered executive briefings conveying complex security concepts to C-suite stakeholders.

BLACKSWAN TECHNOLOGIES LTD | *Israel* — *Feb 2021 – Apr 2023*
Security Architect & SOC Delivery Lead (GRC)

- Implemented MITRE ATT&CK framework across SOC operations, improving detection use cases and client SLA/KPI compliance.
- **Key Projects:** FORTRESS (Zero Trust) | SHIELD (ML threat hunting, SIEM, 1TB+/day) | PHOENIX (DR automation, RTO: 24h→2h). Designed automated pen testing engine reducing testing time by 60%.

VIRTUSA LTD | *Sri Lanka* — *May 2020 – Feb 2021*
Lead Consultant – Security Operations & Infrastructure

- Led 15-member team for Vodafone ISP security transformation. Implemented DevSecOps (Jenkins, Docker, K8s) and WSO2 IAM for 10,000+ users. Reduced deployment vulnerabilities by 80%.

COMMERCIAL CREDIT AND FINANCE PLC | *Sri Lanka* *Sep 2013 – May 2020*

ICT Consultant Level 3 (IT Manager Level)

- Managed IT security budget for 6+ years. Deployed centralized SIEM (500GB+ daily logs). Secured SAP/Oracle ERP (5,000+ users), 200+ ATMs, 500+ POS terminals. Designed HA clustering (99.95% uptime).

GLOBE INTERNET LIMITED | *Malawi, Africa* *Sep 2007 – Jan 2010*

Senior System Engineer

- Architected nationwide ISP infrastructure (8,000+ customers). Deployed IDS/IPS, SOC/SIEM monitoring, and OpenStack hybrid cloud.

ENTERPRISE TECHNOLOGY / QUEENS RADIO MARINE | *Sri Lanka* *Jan 2001 – Sep 2007*

Network System Engineer / Marine Electronics Technician

- Linux/network admin, Cisco firewalls/VPNs, VMware, Nagios monitoring. Key member of SLPA Mega Port fibre optic security project. Earlier: marine navigation, satellite communication, and safety/defence systems.

⌂ ACADEMIC APPOINTMENTS

University	Modules & Focus	Period
University of Wolverhampton, UK	MSc: Incident Management & Response	May 2026 – Present
SLTC Research University, LK	BSc Hons: Cyber Warfare, Blockchain & Applications	May 2025 – Present
Univ. of Gloucestershire, UK	MSc/BSc: Secure Software, Reverse Engineering, ML Malware, IoT, Cloud Security	Sep 2023 – Present
London Metropolitan Univ., UK	BSc Hons: Cloud Security, Network Security, Authentication	Feb 2019 – Jan 2020

⌂ EDUCATION

Qualification	Institution	Year
PhD (Distinction) – Information Security & Forensics	IIC University of Technology	2023–2026
MSc (Distinction) – Network & Info Security	Kingston University, UK	2017–2018
BIT – Information Technology	University of Colombo	2010–2013
Adv. Diploma (Distinction) – Electronics & Telecommunications	City & Guilds of London	2000–2005

◆ KEY INNOVATIONS & SECURITY SOLUTIONS

Solution	Description
AI-Auto SOC Analyst	Replaces time-consuming SOC analyst workload with Advanced AI automation
AI-Cyber Drome	Auto-defends AWS multiple firewalls from real-time attackers
AI-Eagle	Auto-detects credentials across AWS/Azure/GCP/Docker/Git/FS infrastructure
AI-ZeroX	Hybrid ML/AI driven penetration testing platform for network risk assessment
AI-OSX	Auto-identifies source code Patch Management with MITRE/NIST/CVSS validation
AI-Cloud Drome	Auto-validates IaaS audit and performs PoC-level validation for AWS/Azure
AI-MailGardian	Auto-validates email reachability in dark web and provides breach mitigation
AI-AutoPentest	Auto-identifies zero-days and known exploitability of any infrastructure for risk mitigation
AI-Cluster Guard	Auto-manages server environments (ERP, MIS) using AI-driven monitoring and orchestration

☆ RESEARCH PUBLICATIONS (SELECTED FROM 9+ IEEE/PEER-REVIEWED)

- "Hybrid Supervised ML Driven IP Reputation Validating Techniques for Cloud Firewalls" – IEEE, Jun 2025 **(85% false positive reduction)**
- "Hybrid ML for Enhanced Vulnerability Detection in Cloud" – IEEE, Apr 2025 **(60% faster detection)**
- "ML and Moving Target Defence for Switchport Attack Detection" – IEEE, Jan 2025 **(90%+ accuracy)**
- "Multidisciplinary Approaches in AI" – Cambridge Scholars Publishing, Oct 2024 (Book Chapter). Plus 5 additional publications in IEEE, WSEAS, MECS Press, GJCST (2023–2024).

★ CERTIFICATIONS & PROFESSIONAL RECOGNITION

Memberships & Certifications

- MBCS – British Computer Society
- Professional Member – Cybersecurity Division
- RHCE (Trained) | City & Guilds Diplomas
- Data Centre Design | Network Engineering

Awards & Recognition

- IEEE Conference Reviewer/TPC: ICCCNT, ICDCECE, ICARC, icSoftComp, SSITCON
- Certificate of Excellence in Reviewing (2025)
- SLTC External Reviewer (2025)
- Springer Nature TPC Member (2024)

Languages: English (Professional) | Sinhala (Native) | **Programming:** Python (Expert), Shell/Bash, C#, Assembly, SQL

References available upon request.