# NAVIN JAYAWARDENA


+94-712848050
me@navin.dev
navin.dev
https://github.com/Navin47
https://www.linkedin.com/in/navinjay/


## PERSONAL SUMMARY

Security Operations Engineer with a keen focus on fortifying cyber defences. Proficient in crafting and executing custom rules within SIEM platforms, adept at threat detection optimization, and well-versed in monitoring and analyzing diverse logs. Demonstrated expertise in incident response, proactive threat hunting, and continuous fine-tuning of security measures. Committed to maintaining a vigilant cybersecurity posture within a dynamic threat landscape. A Strong team player recognized for fostering a strong team dynamic. Adept at collaboration, actively contributing to a cohesive working environment.

## WORK EXPERIENCE

### ASSOCIATE ENGINEER – INFORMATION SECURITY (SOC)
**2024 June – PRESENT**

CryptoGen (Pvt) Ltd, Colombo Sri Lanka

- Deputy Team Lead of a SOC team of 25 analysts catering for one of the leading private organisations in Sri Lanka.
- Translating information from technical to executive/management terminology on a daily, weekly and monthly basis to communicate SOC status and progress to top-level management.
- Rule logic verification and fine-tuning.
- SIEM asset and log coverage assurance and quantifying through purple teaming in a simulated and live environment. (Aligning to MITRE ATT&CK framework).
- XDR monitoring, response and remediation with of one the biggest companies in the world with 15000+ workstations and servers.
- Threat hunting co-ordination and activities for the above systems.

### Security Operations Centre Analyst
**2023 March – 2024 June**

CryptoGen (Pvt) Ltd, Colombo Sri Lanka

- Contributed to a SOC project for a leading Maldivian bank, enhancing cybersecurity measures and threat protection
- Developed and implemented custom rules in SIEM platforms to enhance threat detection precision and adapt to evolving cybersecurity landscapes.
- Conducted regular fine-tuning of SIEM rules to optimize threat detection accuracy and reduce false positives.
- Conducted proactive threat-hunting exercises to identify and mitigate potential security threats not detected by automated systems.
- Monitoring SIEM in real-time and various client logs were analyzed according to pre-defined rules and procedures.
- Conducted thorough analysis of new alerts within the SIEM, promptly identifying and escalating suspicious findings to respective client for further action within SLA timeframes

### Junior SOC Analyst(Shift Lead)
**2022 Sep – 2023 March**

CryptoGen (Pvt) Ltd, Colombo Sri Lanka

- Led and coordinated security operations during assigned shifts, overseeing the activities of junior analysts to ensure seamless 24/7 coverage.
- Acted as the initial point of contact for incoming security incidents, triaging and assigning tasks to the appropriate team members for investigation and resolution.
- I was able to monitor SIEMs, which were Mcafee and Fortinet.
- Various client logs were analyzed according to pre-defined rules and procedures.
- Any new alerts are taken into consideration, and further analysis was done on these.
- Suspicious alerts resulting from the SIEMs were escalated to the respective clients within the SLA time.
- Apart from SIEMs, the Crowd Strikes EDR Kaspersky Security Center 11 Web Console, McAfee ePolicy Orchestrator Software,Wazuh – The Open-Source Security Platform and Imperva Securesphere were also monitored.
- Conducted comprehensive shift handovers, providing detailed briefings to incoming analysts on active incidents, ongoing investigations, and any notable security events.

**Trainee SOC Analyst** **2022 March – 2023 Sep**

CryptoGen (Pvt) Ltd, Colombo Sri Lanka

- Demonstrated a commitment to continuous learning, actively engaging in ongoing training to stay abreast of evolving SOC technologies and best practices
- Monitored Mcafee and Fortinet SIEMs, analyzing various client logs according to pre-defined rules and procedures.
- Investigate new alerts from SIEMs ensuring thorough analysis before escalating suspicious findings to respective clients within SLA timeframes.
- Monitored Crowd Strikes EDR and WAFs, conducting comprehensive incident and detection investigations before initiating the escalation process.
- Authored detailed threat intelligence reports, delivering actionable insights on emerging threats.

## EDUCATION

**BSc (Hons) in Information Technology Specializing Cybersecurity.** **2020 - 2024**

- Sri Lanka Institute Of Information Technology
- Conducted research and published a paper at the 5th International Conference on Advancements in Computing ICAC 2023 on "Machine Learning Based Web Application Plugin for Threat Detection and IP Analysis"

**Bandaranayake College Gampaha** **2011-2019**

Completed high school education while engaging in Extracurricular activities.

- Completed G.C.E. Advanced Level ( Technology Stream 2019)
- Completed G.C.E. Ordinary Level (2016)

## Extracurricular Activities.

- Vice-Captain of Rugby Team (Bandaranayake College 2017-2019)
- Member of the Rugby Team (Bandaranayake College 2011- 2019)
- Playing Rugby (Since 2011)
- Member of Sport Club (Bandaranayake College 2011-2019)
- Member of Technology Club (Bandaranayake College 2018-2019)
- Member of Gaming Club (Bandaranayake College & SLIIT)

## PROFESSIONAL CERTIFICATES

- Fortinet Certified Associate Cybersecurity
- Chronicle Certified SOAR Analyst (CCSA)
- Chronicle SIEM Fundamentals
- Chronicle SOAR Fundamentals V6 (CSFv6)
- Foundations of Operationalizing MITRE ATT&CK
- CYBER THREAT INTELLIGENCE 101
- ISO/IEC 27001 Information Security Associate™
- Introduction to Cybersecurity (Cisco)
- Cyber Forensics ( Great Learning)
- Intro to Splunk
- CyberSecurity and Oracle Cloud (Oracle)
- Fortinet Network Security Expert Level 1: Certified Associate
- Fortinet Network Security Expert Level 2: Certified Associate
- Fortinet Network Security Expert Level 3: Certified Associate
- SOC Analyst Training with Hands-on to SIEM from Scratch
- Networking Essentials (Cisco)
- Introduction to IoT (Cisco)
- Introduction to Cybersecurity Tools &Cyber Attacks (IBM)
- Cybersecurity Essentials (Cisco)
- Cloud Governance Principles (Crybrary)
- Linux Essentials (Cisco)

## TECHNICAL SKILLS

- SIEM Platforms

(FortiSIEM, Trellix ESM, LogRhythm, Azure Sentinal, Chronicle)

- CrowdStrike Falcon EDR & XDR
- Log Analysis
- Incident Response
- Alert Management
- WAF (Web Application Firewall)
- Threat Hunting
- Continuous Monitoring
- Incident Escalation
- Code Comprehension
- Security Auditing
- Penetration Testing tools
- Report and Documentation
- Threat Intelligence Integration
- Vulnerability Assessment and Penetration Testing (VAPT)

## CORE COMPETENCIES

Strong Leadership Skills, Competent communication skills, Ability to adjust according to the situation (adaptability) and listen to others and accept, Willingness to continuous learning.

## REFERENCES

**Mr. Uvin Rathnayaka**
Manager SOC Oparations
Cryptogen PVT LTD
+94 779688662
uvin@crypto-gen.com

**Ms.Lilani Chandrasekera**
Attorney at Law and Notary Public
No 199, New Kandy Road, Veliveriya.
+94 33 2255074
lilanic62@gmail.com

## Declaration

I hereby declare that the above particulars of facts and information stated are true, correct and complete to the best of my belief and knowledge.

.....

W.A. Navin Jayawardena

01/09/2024