



# Suraj Singh

**Gender:** Male | **Phone number:** (+971) 527091551 (Mobile) | **Email address:**

[surya9900k@gmail.com](mailto:surya9900k@gmail.com) | **LinkedIn:** <https://www.linkedin.com/in/surya9900k/> |

**Address:** Dubai, United Arab Emirates (Home)

## • SUMMARY

I am a highly accomplished information security professional with a distinguished track record and extensive expertise in cyber threat identification, incident analysis, response, and operations. Possessing refined critical thinking skills, I specialize in the meticulous development and enforcement of information security policies that align with recognized industry standards. My comprehensive background includes the execution of thorough security reviews and investigations and the implementation of network defense strategies to fortify organizational security postures. I am actively seeking opportunities within esteemed and forward-thinking organizations where my expertise can be strategically applied to strengthen information security frameworks

## • CORE SKILLS

- Security Incident Management
- Information Risk Assessment
- Familiarity with NIST Framework
- Security Architecture
- Dynamic Malware Analysis
- AQL & (KQL) Kusto Query Language
- Endpoint Detection and Response (EDR)
- SIEM Administration & Monitoring
- Azure-Sentinel, Qradar, Splunk, Azure Defender, Crowd strike & Carbon Black,
- Metrics, Reports, Dashboard
- MITRE ATT&CK Framework
- Use Case Development
- Technical Leadership
- Threat Hunting
- Dynamic Malware Analysis
- Security System Administration
- IT Coordination and Escalation Handling
- Strategy Planning
- Vulnerability Management
- Team Management

## • EDUCATION

2008 – 2012      Kurukshetra University

**Bachelor's Degree, Electronics and Communication Engineering**

## • PROFESSIONAL WORK EXPERIENCE

2021 – CURRENT      Dubai, United Arab Emirates

**SENIOR SECURITY ANALYST**

**DU TELECOM**

- Leading the Security Operations Center (SOC) Analysts team of 10 members, providing clear guidance and direction to optimize team performance.
- Leading multiple Cyber Security Projects, proving consultancy & conducting organization-wide Cyber Security Awareness Programs
- Analyzed security breaches to identify root causes and enhance incident responses and disaster recovery plans.
- Implemented, administered, and operated security technologies to proactively identify, address, and resolve security threats, vulnerabilities, incidents, and events.
- Providing recommendations to management on issues related to information and cyber security
- Showcasing proven excellence in managing end-to-end deployment, implementation and project consulting functions.
- Developed and implemented rules and use cases to support incident response strategies aligned with business needs.
- Participated in projects as an information security Subject Matter Expert (SME), analyzing solutions, processes, and infrastructure, and providing recommendations for information security controls implementation and incident management.

2019 – 2021      Dubai, United Arab Emirates

**SECURITY ANALYST II**

**SECURITYHQ**

- Analyzed, identified, and effectively managed information security incidents, ensuring a swift and efficient response.
- Demonstrated proficiency in performing general forensics and malware analysis.
- Implemented Advanced Persistent Threat detection and response tactics, techniques, and procedures.
- Conducted proactive threat hunting activities to strengthen security posture.
- Authored reports, providing valuable insights into the effectiveness of existing security policies, incident response strategies, disaster recovery plans, and other security-related information.

- Strong understanding of various technologies, including Windows, Linux, network devices (WAF, Firewalls, Switches), cloud, and application logging.

2018 – 2019 Gurgaon, India

#### INFORMATION SECURITY ANALYST

FIS GLOBAL

- Led efforts to proactively counter security breaches, employing advanced techniques and regulatory requirements to anticipate and reduce the likelihood of future security threat alerts, incidents, and disasters.
- Created, implemented, and meticulously maintained security protocols and controls, ensuring the safeguarding of digital files and data against unauthorized access.
- Ensured the security systems were consistently up to date, employing the latest technologies and best practices to maintain a strong customer relations support and effectively managed security incidents.
- Managed network intrusion detection systems, actively monitoring security access and maintaining essential data for analysis

2017 – 2018 Gurgaon, India

#### SERVICE DESK ENGINEER

CVENT, INDIA

- Provided IT Infrastructure field support, adeptly troubleshooting hardware, software, and OS issues while maintaining hardware warranties and security compliance.
- Demonstrated hands-on proficiency in installing, diagnosing, and resolving hardware problems for desktops, laptops, printers, and computer peripherals.
- Possessed basic knowledge of enterprise LAN and WAN setups, executing smart hand activities per instructions at various sites.
- Skilled in desk-side support, including PC break/fix and Windows OS administration, ensuring seamless operations.
- Utilized Anti-spyware and Anti-virus software, maintaining robust security measures for systems and networks.

2016 – 2017 Gurgaon, India

#### ANALYST

HCL TECHNOLOGIES

- Led the capture, validation, logging, and prioritization of service requests and issues of IT Hardware and Software.
- Orchestrated initial triage and provided prompt solutions within agreed SLAs.
- Effectively communicated status updates and monitored issues to closure.
- Contributed to knowledge base articles, sharing knowledge to improve troubleshooting workflows for incidents and event.

## CERTIFICATIONS

09/2023 – 09/2026

#### Certified Information Security Manager

ISACA

09/2023 – 09/2026

#### Azure Fundamentals

Microsoft

09/2023 – 09/2026

#### COMPTIA (SECURITY+ | CYSA+ | CSAP)

COMPTIA

06/2022 – 07/2025

#### ISO 27001 LEAD AUDITOR & LEAD IMPLEMENTER

ISO CERTIFICATION

10/2021

#### IBM CERTIFIED CYBER SECURITY ANALYST

IBM COURSERA

04/2020

#### QUALYS VULNERABILITY MANAGEMENT & POLICY COMPLIANCE SPECIALIS

QUALYS