Pukhraj Singh

Threat Intelligence | Cyber Geopolitics | Writing
Gurgaon, Haryana, India

Summary

I am a technically grounded, senior cyber threat intelligence
professional with more than a decade of experience. My career
spans national government agencies, start-ups and global response
teams in India, Canada, the US and Israel.

Keywords: Cyber threat intelligence, geopolitical analysis, security
operations, incident response, disinformation, and public policy

Skill sets:
- Aligning a technical understanding of cyber threat intelligence with
business and strategic objectives.
- Blending complex geopolitical events with the technical facets of
cyber intelligence.
- Incubating security product/solutions architecture from ground-up,
covering the end-to-end business cycle.
- Tracking threat actors to build a larger picture of their remit,
incentives, limits and other boundary conditions.
- Providing strategic guidance on security operations and incident
response.
- Awareness of modern threat analytic frameworks like ATT&CK,
CAPEC, STIX 2.1, Cyber-F3EAD, Diamond Model, and NIST 800-X,
etc.

Experience

Bhujang Innovations
Director, Cyber Threat Intelligence
April 2016 - March 2019 (3 years)
Gurgaon, India

Bhujang was a homeland security venture led by Vice Admiral DSP Varma, the
former DG of the Indian nuclear submarine programme. It was a cyber security
solutions engineering company -- prototyping threat intelligence aggregation
and situational awareness platforms. I was also leading the effort to introduce

inter-operable and automated security standards like STIX/TAXII and OpenC2 in India.

Verint
Solutions Leader - Cyber Intelligence
January 2015 - March 2016 (1 year 3 months)
Gurgaon, India

I handled the business development and solutions engineering initiatives of the cyber intelligence platforms division of Verint in India. It is an Israel-based global leader in communications intelligence.

Unique Identification Authority of India (Aadhaar)
National Cybersecurity Manager
October 2013 - December 2014 (1 year 3 months)
New Delhi Area, India

I was the first security manager for the largest digital identity project in the world, responsible for protecting the personally identifiable information of 1.2 billion Indians.

National Technical Research Organisation, Prime Minister's Office
Scientist 'C'/Deputy Director
January 2009 - September 2013 (4 years 9 months)
New Delhi Area, India

I played an instrumental role in the setting up of the cyber defence operations centre of the Indian government. I was laterally inducted into the government after the 26/11 terror attacks. It was a multi-disciplinary tenure ranging from geopolitical doctrine formulation – eventually approved by the Prime Minister – to the very brass-tacks of cyber operations.

I was also a member of seminal government initiatives like National Critical Infrastructure Protection Centre (NCIIPC), Inter-ministerial Task on Cyber-Defence & Preparedness and Information Security Guidelines & Procedures of the Ministry of Home Affairs, etc.

It was a worthwhile opportunity to pay back my dues to the nation.

Symantec Canada
Senior Threat Analyst
November 2006 - September 2007 (11 months)
Calgary, Canada Area

I was an analyst and a researcher with DeepSight, industry's first Internet-wide threat intelligence service.

Third Brigade (acquired by Trend Micro) & Blue Lane (acquired by VMWare)
Manager/Security Researcher
July 2004 - June 2006 (2 years)
Ottawa, Canada Area

I had two short tenures with intrusion prevention product start-ups, Third Brigade (based in Canada; acquired by Trend Micro) & Blue Lane (based in Pune, India; acquired by VMWare)

Education

Punjab Technical University
B.Tech, Information Technology · (2000 - 2004)