Prasanth Natarajan

Cyber Security Architect | Splunk Consultant | SOC Manager | Corporate Trainer

Chennai,Tamil Nadu,India - +91.94424 49804 - mail2prasanth1996@gmail.com
https://www.linkedin.com/in/prasanthpro/

Summary

Accomplished and highly organized **Cyber Security Architect** with several years of rich experience in below domains:

- Cyber Incident Response Team -SOC Operations - Splunk 2x Certified
- Security Control Implementations - **Firewalls / IDS-IPS Tools / SIEM / DLP / EDR / Email Gateway**
- Vulnerability Assessments and Penetration testing - **Nessus/Qualys/W3af/Acunetix**
- Cloud Security - **Microsoft Azure 3x Certified**
- Desktop Server support - **SCCM, MDT**
- Malware Analysis - **Autopsy, IDA Pro, Encase**
- Cyber Threat Intelligence - **MITRE ATT@CK/D3fend Feed integrations**

I have ethically **reported many security vulnerabilities** to companies like **Audi, Bentley, InVision, Western Union, Indeed** and got Acknowledged and Rewarded by them.

Education

Bachelor of Engineering / Bachelor of Technology, Electronics and Communication Engineering	2017/06
SASTRA University	Completed

Work Experience

Cyber Security Engineer	October 2017 - May
Tata Consultancy Services	2018

As part of Cyber Infra team that was responsible for maintaining a large IT infrastructure environment, I got hands-on experience of managing virtual machines and physical

Skills

- Security Operations Center (SOC) - Monitoring and Management
- Splunk Admin/Developer/Enterprise Security
- Splunk 1001 & 1002 Certified
- SIEM - IBM QRadar/ELK Stack/Azure Sentinel
- CompTIA Security+ Certified
- MITRE ATT@CK Certified Defender
- Penetration testing - WebApp, Mobile, Network, Blockchain
- Network Security Tools Implementation
  - Firewalls - Palo Alto, Forcepoint, FortiGate
  - IDS/IPS - SNORT, OSSEC
  - NAC - PacketFence
  - Proxies - Bluecoat, Zscalar
- Endpoint Security Tools Implementation
  - AV - Sophos/McAfee
  - EDR - Crowd Strike, Cortex XDR
- Phishing Email investigation - SPF, DMARC, DKIM Analysis, Proofpoint, Knowbe4
- Handle ITSM incidents - Service Now
- Cloud operations - 3x Azure Certified, AWS, GCP
- Malware Analysis - Process Hacker, IDA Pro
- Windows Server Ops - ADDS, DNS, DHCP
- IAM Tools - SailPoint, OIM, OAM
- SSO - Ping Federate, Okta, CyberArk

Training & Certifications

- CompTIA Security+ Certified - SY0-501, 2020
- Splunk Core Certified User - SPLK 1001, 2021
- Splunk Core Certified Power User - SPLK 1002, 2021
- Critical Infrastructure Protection Specialist, US - Department of Homeland Security, 2021
- Microsoft Azure Certified - AZ 900, AI 900, DP 900, 2021

machines in VMware and MDT(SCCM) and performed L2 administrative tasks.

- Strong knowledge and demonstrable experience of **Information Security Technologies and Methods**
- Implemented and managed the **Airgap network** for TCS internal teams with all **Defense in Depth tools** in place
- Configuration, Administration, Troubleshooting of **Windows Server 2016** (Windows Server Update Services, Active Directory Domain controller, DHCP, DNS, Containers)
- Installation, Configuration and management of **Microsoft Deployment Toolkit**, **System Center Configuration Manager**
- Configured and managed **SIEM, Log Vaults, CASB, VPN** Connections for various teams
- Implemented various network security tools (**Packetfence** for NAC), Vulnerability scanners (**Nexpose, Nessus, W3af, Acunetix Qualys**)
- Various security consultations were given for team members to **make their Webapp/Networks 100% Compliant**
- Performed various Penetration testing operations for Network and web applications and mitigated the issue
- Had a hands-on knowledge of Containers (**Dockers), DevOps tools (Chef/Puppet/Ansible) and GIT**

Security Operations Center - Manager May 2018 - Current

Tata Consultancy Services

Currently, I have been working as **Security Operation Center (SOC) - Manager** for one of the famous banks in Chicago to help their infrastructure safe from malicious threats.

- Performed the Installation, configuration of **SPLUNK** instance - **UF, Indexes, Search head Clustering, Deployer, Cluster master** configuration tasks
- Configured Splunk-**Enterprise Security Modules** and created many **Correlation searches/Adaptive responses/Workflow Actions** responsible for detecting security and health incidents

- Exploitation With Kali Linux, CodeRED - EC-Council, 2020
- Phishing Email Countermeasures Certified, Charles Sturt University, 2020
- Fortinet Network Security Associate, 2022
- CISSP - To be Completed by 2022, 2022

Computer Proficiency

Operating Systems

- Windows ●●●●
- Kali Linux ●●●●
- ParrotSec ●●●○
- *NIX ●●●○

Softwares

- Splunk ●●●●
- MS Office APPS ●●●●
- Azure ●●●○
- Docker ●●●○
- SCCM/MDT ●●●○
- Burpsuite/ZAP/Metasploit ●●●●
- Proofpoint TAP ●●●○
- Cisco Umbrella ●●●○

Language

- English ●●●○
- Tamil ●●●●

Personal Interests

- Bug Bounty Hunting
- Playing CTF's
- Taking Cyber Security trainings/mentoring people
- Table Tennis

Personal Information

Birthday:	02/05/1996
Marital Status:	Single
Gender:	Male
Nationality:	Indian
Address:	4-12, Chetty Street Mela Kabisthalam Chennai - 614203 Tamil Nadu India

Declaration

Prasanth Natarajan Chennai, Tamil Nadu

- Created complex **Rules, Dashboards, Building Blocks, Reference Data & Scheduled Reports in Splunk**
- Configured 50+ **Splunk detection rules** on Splunk Enterprise Security and tuned the false positives
- Investigated breached incidents using **SPL queries, pattern analysis and various reports**. Triaged Security events and Incidents detect anomalies and report remediation actions
- Provided much **real-time guidance to customers** on network configuration, security settings and policies, and attack mitigation procedures
- Having good process knowledge in **ITIL** practices such as handling Incident, Change and Service management requests - Experience in Service-Now and Ivanti HEAT ITSM tools
- Hands-on in **Proofpoint Email Security Gateway tool** - Continuous monitoring and analyze the active, mitigated, blocked and suspicious Email threats in TAP dashboard
- Analyzing **Phishing/Vishing/Fraud Emails** of the reported users within the prescribed SLA
- Having a hands-on knowledge of **Firewalls/Proxies/IDS-IPS** devices
- Having Handson experience in **DFIR - Autopsy tools, Joe Sandbox, Hybrid Analysis** for malware analysis and remediation
- Having in-depth knowledge in Identity Governance**/IdM/IAM/PAM tools like SailPoint/Ping Federate/Okta/CyberArk**