Naveen raj

naveenselvaraj1997@gmail.com | Linkedin: naveend3v

ABOUT ME

As a CyberSecurity enthusiast, who loves to work in cloud security and has strong knowledge of cloud security fundamentals to defend cloud environment threats from misconfigurations and attacks, and good experience in analyzing threat detection via logs and threat behavior patterns.

CERTIFICATIONS

Certified Ethical Hacker - CEH

Ec-Council | Cert ID: ECC2537691084

Google Cloud Certified Cloud Digital Leader

Google | Cert ID: SVHiDb

AWS Cloud Practitioner Essentials

AWS | Cert Link: Click here 🔗

Foundations of Operationalizing MITRE ATT&CK

AttackIQ | Cert Link: Click here 🔗

Splunk 7.x Fundamentals

Splunk | Cert Link: Click here 🔗

SKILLS

Cloud
• AWS cloudtrail, VPC, EC2, S3, EBS, RDS, SNS, SQS • Alibaba OSS, ActionTrial, Log service

SIEM Tool
• Splunk • AIsaac MDR

Log Management Tool
• ArcSight • Apache Druid

Programming
• HTML • CSS • JavaScript

VAPT Tools
• Nmap • Metasploit • Wireshark
• Hashid • Wpscan • Hashcat • Amass
• SQL Map

Operating System
• Linux (ubuntu, kali)

Vulnerability Assessment Tools
• Nmap • Nessus

LINKS

GitHub:// naveend3v
LinkedIn:// naveend3v

EXPERIENCE

SECURITY ANALYST - Atos

Sep 2021 - Present | Bangalore, India

- Analyzing logs of the various software products like firewalls, switches, cloud, and database services and collecting, parsing, and transforming logs from raw log to CEF fields and using it for AIsaac MDR for monitoring and detecting threats and log analysis in ArcSight and Druid logger
- Monitoring Cloud environments using AWS - cloudTrail, Alibaba - ActionTrail, GCP - Admin Audit and Data access logs for logs services like VPC, EC2, S3, Route53, AWS RDS, load balancers, OSS, WAF, SecurityCenter, etc and Kubernetes platforms and detecting threats by creating SIEM rules from these logging resources.
- Monitoring and detecting threats in real-time threats like log4j etc and their exploitation attempts by researching their behaviors and Indicator of Compromise (IOC) using SIEM rules and Threat Hunting models like VPC, IDS, IPS, DNS, etc.

SUPPORT AND MONITORING ENGINEER - Tomia

Jun 2021 - Sep 2021 | Bangalore, India

- Analysed complex service-related problems and configurations and recommended solutions accordingly in Windows servers and the MSSQL database.
- Handled bulk system user account maintenance on the windows server.
- Prepared server health and transaction reports and monitored tickets in Zendesk from clients and troubleshoot them in priority without affecting SLA.
- Monitored the Client's server's health and disk usage with the PRTG tool in real time.

EDUCATION

KALASALINGAM UNIVERSITY - Virudhunagar, India

B.Tech in Civil Engineering
Grad: May 2018 | CGPA 6.24

NAMMHSS SCHOOL - Theni, India

PCM with Computer Science
Grad: April 2014 | Cum Per: 82 %

PUBLICATIONS

How I passed the Google Certified Cloud Digital Leader exam 🔗
How I Passed AWS Certified Cloud Practitioner Exam 🔗