Ojasvi Ashish Chauhan *Senior Threat Detection Engineer*

ojaschauhan44@gmail.com

+918627000279

India

https://www.linkedin.com/in/ojasviashishchauhan

https://github.com/ojasviashishchauhan

https://www.kaggle.com/ojaschauhan44

Profile

Passionate Cyber Security Engineer with strong scripting skills and expertise in Information Security, Automation, Incident Response, and Security Analytics. Focused on securing high-availability infrastructures through creative solutions. Skilled at threat detection and response, security infrastructure deployment through IAC & managing team of security experts. Experienced in enhancing security practices and making operations more efficient.

Professional Experience

2021/07 – present

Senior Threat Detection Engineer
Tide Platforms Ltd

- Leading log management for SIEM solutions' like Splunk, Chronicle, and S3, including developing parsers' and normalization techniques for various log formats.
- Building and deploying advanced threat detection models / queries to enhance security, focusing on identifying true positive alerts and reducing false positives.
- Leading initiatives to develop insider threat detection programs by analyzing user behavior and implementing anomaly detection.
- Building and deploying machine learning (ML) and artificial intelligence (AI) models to enhance detection capabilities.
- Deploying and configuring data & threat centric security tools such as MISP, Proofpoint TRAP, and Osquery for threat intelligence and security.
- Mentoring and managing a team of 7 to keep company's overall infra secure.
- Administering Splunk SOAR and Chronicle SOAR tools to create playbooks / runbooks and automate incident response processes'.
- Experienced in working with Amazon Web Services (AWS).

2019/01 – 2021/07

Cyber Security Engineer - II
Fair Isaac and Corporation (FICO)

- Implementation of Infrastructure as Code (IAC) using terraform to automate the deployment and management of infrastructure componets.
- Utilization of SIEM to create use cases for monitoring diverse platforms, with a focus on refining these to get relevant alerts.
- Management of AWS environment, encompassing security service such as Guard Duty, Lambda, S3, Cloud Trail, Cloud Forensics and integration with DecSecOps practices.
- Incident response to security alerts by triaging alerts from multiple sources including Endpoint Detection and Response system like Windows ATP and Cylance, Splunk, Web Proxy , Demisto SOAR.

Education

2024/01 – 2025/06

Advance Management Program in Business Analytics
Indian School of Business

2023/01 – 2024/04

Masters in Cyber Security
Indian Institute of Technology, Kanpur

2015/07 – 2019/06

Bachelor's of Engineering CSE
Chitkara University, Punjab

Skills

Technical Skills — Python, Machine Learning, JavaScript , C , SOAR, Splunk, AWS, Terraform, Proofpoint, Zscaler, Google SIEM & SOAR, Fleet Osquery, Tableau, Apache Sparks, Data Bricks, PyTorch, Scikit Learn, Incident Response

Certificates

- Aws Certified (Solution Architect & Security Specialty)
- Simplilearn Certified (Data Science with Python & Machine Learning)
- Udemy Certified (Full Stack Developer, Docker, Terraform, AWS Lambda & serverless, DevSecops, Machine Learning)
- Proofpoint Certified (Insider threat Specialist, Security Awareness Specialist, Identity threat Specialist)

Projects

Vulnerability Management — Osquery to rescue
When facing challenges with vulnerabilities in the company, developed a solution to utilize open-source tools, specifically fleet-Osquery, to gather software intelligence and identify vulnerabilities and also designed an automated process that would notify the IT team about vulnerabilities and close the case once it was patched.

Insider Threat Program — Leveraging data Science
Every fintech company faces the issue of insider threats, where sensitive information can be leaked by an internal employee. To monitor and detect this, designed an ML model based on the isolation forest algorithm, achieving an accuracy of about 73%.

Securing Customer Card data leak's
Utilizing threat intelligence and open-source data, we gathered and analyzed information on compromised card details from various online sources, including dark web forums, hacker marketplaces, and breached databases, and then took proactive measures to prevent scams and fraud.

Achievements

6-time FICO Spot Award Winner

Speaker @ Splunk Conference 2022

2-time Tide Star Award Winner