

Sai Chaitanya Jasthi

(438) 926-6567 | jasthichaitanya567@gmail.com | [Linkedin](#) | [Github](#)

SUMMARY

I excel in performing efficiently under high-pressure scenarios, conducting in-depth analyses of security incidents, offering mentorship to incoming team members, and fostering robust collaborative connections with peers.

PROFESSIONAL EXPERIENCE

SecureOps

Montreal, QC

Cyber Security Analyst

Oct 2021 - Dec 2023

- Monitored network activities daily, investigating incidents and collaborating with senior analysts to handle complex incident response processes, resulting in a 15% reduction in false positive alerts.
- Utilized SIEM tools such as **Splunk**, **Sentinel**, and **ArcSight** for in-depth analysis of security incidents, successfully identifying the root cause and implementing necessary measures to prevent future occurrences.
- Effectively employed both **JIRA** and **ServiceNow** tools as integral components of the security incident management process. This approach facilitated streamlined communication, swift issue resolution, and comprehensive documentation of incident handling procedures.
- Generated comprehensive reports outlining investigation findings, providing valuable insights for the improvement of security protocols and risk detection rules.
- Conducted thorough investigations of Web proxy/Firewall alerts, including **Zscaler** and **Imperva**, to thwart application layer attacks.
- Conducted detailed investigations with **FireEye** and **SentinelOne** Endpoint Security tools to identify and mitigate potential cyber threats.
- Examined and addressed **Microsoft Defender for Cloud**, and **Microsoft Defender for Endpoint** security alerts, leading to a notable reduction in potential security risks.
- Identified and assessed cyber risks across multiple instances, resulting in the development and implementation of best practice solutions for mitigating those risks.
- Monitored and analyzed security alerts from multiple systems including Intrusion Detection & Prevention Systems (**NIDS/NIPS**), Log Monitoring, File Monitoring, and SIEM for a range of business-critical devices, resulting in a substantial reduction in potential security breaches.
- Proficient in conducting comprehensive investigations of alerts within **Azure** and **AWS** environments, leveraging in-depth knowledge of cloud security protocols and incident response methodologies.
- Conducted proactive **Threat hunting** activities using customized intelligence targeting clients in specific industries.

MP Police State Cyber Cell

Madhya Pradesh, India

Data Forensic Intern

May 2019 - Jun 2019

- Utilized advanced hardware such as **Cellebrite Universal Forensic Extraction Device** and custom mobile forensic tools to extract images of data hierarchy from computing and mobile devices, resulting in obtaining crucial evidence for ongoing investigations.
- Performed in-depth analysis of disk images using open-source tools **FTK Imager** and **Autopsy**, resulting in the identification and extraction of evidence.

ByodBuzz

Andhra Pradesh, India

Security Analyst Intern

Apr 2018 - May 2018

- Conducted comprehensive vulnerability assessments on the company's web applications, identifying and remediating **XSS** and **SQL** injection vulnerabilities.
- Performed network analysis using **Nmap**(NSE) to identify potential weak points and security enhancements.
- Utilized hands-on experience with vulnerability analysis tools including **Burp Suite** and **OWASP Zap** to test and identify web application vulnerabilities.

EDUCATION

ISI, L'institut Supérieur d'Informatique
Postgraduate Diploma (Computer Networks and Security)

Montreal, QC
Graduation Date: Sep 2021

PVP Siddhartha Institute of technology
Bachelor of Technology (Computer Science and Engineering)

Vijayawada, AP
Graduation Date: Apr 2019

SKILLS

Strong understanding of computer networking concepts, Incident Investigation, Malware analysis, Security

Skills: Operations, Complex Problem Solving, Regex, and Microsoft Office (Excel, Word, PowerPoint).

Languages: C, Python, Powershell

Tools: Microsoft 365 Defender enterprise suite, Splunk, ServiceNow, Jira, Qradar, FireEye HX, SentinelOne, Wireshark, MITRE ATT&CK Framework, Zscaler.

PROJECT EXPERIENCE

Personal AWS project Oshawa, ON
Cloud Resume Challenge *Jan 2024 - Jan 2024*

- Established website hosting on Amazon S3, utilizing CloudFront for optimized network flow. Implemented secure access to S3 resources with Origin Access Control (OAC) configuration. Employed Amazon Certificate Manager (ACM) to generate and manage SSL/TLS certificates for the website domain.
- Implemented a visitor count feature on the website, utilizing DynamoDB to store and retrieve the count value through a Lambda function. Configured API Gateway to accept requests from the web application, triggering the associated Lambda function securely.
- Streamlined the development workflow by harnessing the power of GitHub Actions. Automated the process of updating and deploying code changes to enhance efficiency and maintain a seamless development pipeline.

ISI, L'institut Supérieur d'Informatique
Network design

Montreal, QC
Feb 2021 - Mar 2021

- Planned and executed the development of a resilient computer network infrastructure, incorporating primary and secondary DNS servers, a Linux web server with CMS, firewall, load balancer, and Snort IDS/IPS system.
- Set up a PfSense firewall alongside an open-source load balancer (VAProxy) for efficient workload distribution across multiple web servers. Integrated Snort for comprehensive network monitoring and intrusion detection/prevention.
- Implemented robust access controls and protocols to guarantee the accessibility of the web server situated in the DMZ from both the Internet and Intranet, ensuring secure connectivity.

CERTIFICATIONS

- SBT Blue team Level 1
- CompTIA Cysa+, Security+
- AWS Certified Solutions Architect Associate
- CompTIA Security Analytics Professional – CSAP Stackable Certification
- Microsoft Certified: Security Operations Analyst Associate (SC-200)
- Certified Ethical Hacker (CEH)
- Splunk Certified Cybersecurity Defense Analyst