Sai Chaitanya Jasthi

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

SUMMARY

I am proficient in functioning effectively within high-pressure environments, conducting thorough investigations into security incidents, providing guidance to new team members, and establishing strong collaborative relationships with colleagues.

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.
- Utilized **JIRA** and **ServiceNow** tools to track and manage security incidents.
- 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.
- Trained and mentored new team members.
- 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 Supérieurd'Informatique **Montreal, QC**
Postgraduate Diploma (Computer Networks and Security) *Graduation Date: Sep 2021*

PVP Siddhartha Institute of technology **Vijayawada, AP**
Bachelor of Technology (Computer Science and Engineering) *Graduation Date: Apr 2019*

SKILLS

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

ISI, L'institut Supérieurd'Informatique **Montreal, QC**
Network Design *Feb 2021 - Apr 2021*

- Designed and implemented a fault-tolerant computer network infrastructure, including primary and secondary DNS servers, Linux web server with CMS, firewall, load balancer, and Snort IDS/IPS system.
- Configured a PfSense firewall with an open-source load balancer (VAProxy) to effectively distribute workloads among multiple web servers and implemented Snort for network monitoring and intrusion detection/prevention.
- Ensured accessibility of the web server located in DMZ from both the Internet and Intranet by implementing secure access controls and protocols.

CERTIFICATIONS

-SBT Blue team Level 1

-CompTIA Cysa+, Security+

-AWS Certified Solutions Architect Associate

-CompTIA Security Analytics Professional – CSAP Stackable Certification

-Microsoft Certifed: Security Operations Analyst Associate (SC-200)

-Certified Ethical Hacker (CEH)

-Splunk Certified Cybersecurity Defense Analyst