Chatti Siva Kumar

SOC Analyst – Cybersecurity Enthusiast
Hyderabad, Telangana, India

✉ chatti.shiva.tu@gmail.com ☎ +91-9502185447 LinkedIn GitHub Portfolio Website

SUMMARY

SOC Analyst with hands-on experience in SIEM monitoring, log analysis, and incident response using Microsoft Sentinel and Splunk. Skilled in investigating security alerts, performing incident triage, and escalating threats based on severity. Proficient in proactive threat hunting using KQL and SPL, correlating security events, and mapping adversary techniques to the MITRE ATT&CK framework. Experienced in log ingestion, parsing, and optimizing detection rules to enhance threat visibility while reducing false positives. Adept at configuring dashboards, refining correlation rules, and automating SOC workflows using playbooks and scripting to improve response efficiency.

PROFESSIONAL EXPERIENCE

Application Security Engineer Intern, Next24Tech Apr 2024 – May 2024

- Developed and secured an Online Voting System, ensuring authentication, authorization, and data integrity.
- Performed security testing on web applications and APIs, identifying vulnerabilities such as SQL Injection, XSS, and authentication flaws.
- Analyzed backend security configurations, API security policies, and session management to detect potential threats.
- Developed Python-based automation scripts using Selenium to streamline security testing and vulnerability detection.
- Assisted the team with API integration and backend security, ensuring proper authentication, authorization, and data validation.

Junior SOC Analyst – Internship, Verzeo Edutech Jul 2023 – Aug 2023

- Conducted OSINT investigations to gather intelligence on potential threats and improve security awareness.
- Assisted in simulating attack scenarios to understand cyber threats and identify security weaknesses.
- Analyzed phishing emails and malicious attachments, identifying indicators of compromise (IoCs).
- Used Linux-based tools for web application security testing, focusing on OWASP Top 10 vulnerabilities.
- Prepared detailed reports and documentation, summarizing findings from security assessments and investigations.
- Reviewed log data and security alerts, identifying unusual patterns and potential threats.

SKILLS

- SOC & Security Monitoring: Microsoft Sentinel, Splunk, Defender XDR
- Threat Detection & Response: KQL, SPL, MITRE ATT&CK,
- Incident Detection and Response: IDS/IPS, EDR
- Security Automation : Python, Bash, Splunk SOAR, Sentinel Logic Apps, Automated Incident Response Workflows
- Dashboard & Rule Management : SIEM Correlation, Alert Optimization, Custom Rule Creation, Event Filtering
- Log Ingestion & Parsing: Firewalls, Endpoints, Cloud Services, Custom Log Parsing
- Pentesting & Security Testing: Web, API, and Network Penetration Testing
- Mobile Application testing: APKtool, MobSF, ADB, Drozer, Frida, Qark
- Malware Analysis & Forensics : Threat Intelligence, Digital Forensics, Reverse Engineering
- Cloud & System Security: Azure Security, AWS Fundamentals, Terraform, Windows and Linux Security Hardening, Arch Linux, Packet Tracer
- Development & Scripting : Full-Stack Development, API, Python and Bash

PROJECTS

Incident Documentation and Playbook Development

- Monitored and analyzed security events using Microsoft Sentinel to detect potential threats and anomalies.
- Investigated security alerts, assessed severity, and escalated confirmed incidents to L2/L3 analysts.
- Performed threat hunting using KQL (Kusto Query Language) and Splunk SPL to identify hidden threats.
- Created and optimized dashboards, correlation rules, and alerts to improve threat visibility.
- Ensured proper logs and parsing from firewalls, endpoints, and cloud sources, troubleshooting issues as needed.
- Mapped incidents to the MITRE ATT&CK framework to analyze attack techniques and improve defenses.

Face and Fingerprint-Based Authentication System

- Developed a secure and innovative authentication system using Flask for the backend and machine learning for facial recognition.
- Integrated fingerprint-based access control to provide users with multiple secure login options.
- Addressed and mitigated potential vulnerabilities through comprehensive security testing and debugging.
- Enhanced user experience by creating a simple yet effective interface for credential management and recovery.
- Implemented multifactor authentication (MFA) to further strengthen security and protect user accounts.

Graphical Password Authentication Using Cued Click Points

- Designed an image-based graphical password system that improves both usability and security for end users.
- Developed algorithms to ensure the randomness of click points, minimizing hotspot vulnerabilities.
- Conducted thorough usability testing to validate the effectiveness of the system in real-world scenarios.
- Created detailed documentation to assist future developers and researchers in further enhancing the system.
- Incorporated encryption techniques to securely store graphical password data, ensuring privacy and compliance.

CERTIFICATIONS

- ISC2 Certified in Cybersecurity (CC)
- Cisco CCNAv7: Introduction to Networks
- Cisco CCNAv7: Switching & Routing Essentials
- Introduction to Splunk
- Certified Junior SOC Analyst - TryHackMe
- NPTEL Ethical Hacking Certification
- JNTUH Cyber Forensics Workshop
- Git training - Simplilearn

EDUCATION

B.Tech in Cyber Security 2024
Hyderabad Institute of Technology and Management

Intermediate (MPC) 2020
Narayana Junior College

SSC 2018
Kendriya Vidyalaya Picket

ADDITIONAL INFORMATION

- Completed 20+ Capture the Flag (CTF) challenges, demonstrating problem-solving skills in cybersecurity.
- Reported 10+ security vulnerabilities, earning recognition in Hall of Fame listings.