

NITHINRAJ BUNNI

Hyderabad | +91 9063793006 | bunninithin1007@gmail.com

SUMMARY:

Overall 8 years of experience in SOC IT industry (Including 3 Yr's Non -IT) under the domain Information and Cybersecurity as an incident responder and SOC Analyst with good experience on multiple SIEM tools and EDR tools and have deep knowledge on identifying and analysing suspicious events and network incidents, experienced in various tools to perform log analysis, Can perform malware analysis and threat analysis with overall objective to ensure confidentiality, integrity and availability of systems, network and data.

PROFESSIONAL EXPERIENCE:

Senior Associate (L2 Analyst): 02/2021 to Current.

STATE STREET CORPORATE SERVICES.

Responsibilities:

- Real-time Incident and log monitoring in the Security Operations Centre from different devices such as firewalls, IDS, IPS, and Antivirus and EDR, operating systems like Windows, Linux, and Networking Devices.
- Handle the complete incident management framework cycle right from incident identification, incident containment, performing root cause analysis, suggestion and implementation of preventive and corrective controls and perform network analysis as needed on a case-to-case basis.
- Perform technical investigations and RCA and recommend remediation techniques for the true positive incidents and prepare SOPs for the resolved issues.
- Detailed phishing Analysis with email containing malicious files and URL's.
- Experience in Qualys Vulnerability management tool to perform the Vulnerability scanning, reporting.
- Escalating the security incidents based on the client's SLA and providing meaningful information related to security incidents by doing in-depth analysis of event payload, providing recommendations regarding security incidents mitigation techniques.
- Preparation of incident analysis reports based on daily checklists and monthly reports for clients, including top virus-infected machines, top vulnerabilities.
- Experienced in documenting and analysing incident timelines and events and get involved in reviewing and analysing user access logs to identify unauthorized or suspicious events.
- Experienced SOC analyst in – Microsoft ATP Defender & Crowd strike falcon, Splunk SIEM. on daily basis in rotational 24/7.

- Investigating, analysing events in Endpoint Detection and Response Tool, and then taking required action and making sure tickets are being resolved within SLA.
- Always keep software to the latest version to avoid vulnerabilities and bugs.
- Utilized MS Defender, McAfee, and SEPM for endpoint detection and response, ensuring swift identification and mitigation of security threats.
- Expertise in cyber-attack methods, performing security logs analysis, and providing daily reports to SOC Lead.
- Perform information security incident response based on risk categorization in accordance with established procedures.

Security Analyst: 02/2017 to 11/2020.

BROADRIDGE.

Responsibilities:

- Patched firmware on 40+ device company-wide, which helped increase security by 91%.
- Increased customer satisfaction to 4.5 of a star rating by reducing average ticket time and overhauling the help desk.
- Installed Windows 11 on 30+computers, which helped improve employee performance by 67% YoY(Year over Year).
- Monitored system performance 24/7/365 with tools and successfully maintaining 192% uptime.
- Streamlined the data retrieval by applications, which reduced 43% of network traffic and boosted throughput by 33%.
- Provided personal support to 1200+ users remotely using SysAdmin commands with 94% efficiency.
- Registered customers via QR Code into a tracking database, reducing manual entry by 60%.
- Trade Settlements and Reconciliations:
 - Executed pre-matching techniques to guarantee timely trade settlement on designated settlement dates, optimizing operational efficiency. Instructed delivery trades, matched and approved trades on the DTC system, ensuring seamless transaction processing.
- Trade Capture and Analysis:
 - Leveraged comprehensive experience in trade capture & analysis, ensuring accuracy and completeness of trade data across diverse domestic and international markets. Implemented robust trade validation techniques to mitigate transaction reporting risks and ensure regulatory compliance.

SKILLS:

- **SIEM:** Microsoft Azure Sentinel, ELK Kibana, Q-radar. Splunk.
- **Endpoint Solution:** CrowdStrike Falcon, Microsoft defender 365, Microsoft defender for identity.
- **AV:** McAfee.

- **Data loss prevention (DLP):** Zscaler, Symantec DLP.
- **Vulnerability Management tools:** Nessus, Qualys.
- **Ticketing Tools:** ServiceNow.
- **Threat Intelligence:** Virus total, URL Scan, IP Void, Cyberchat.
- **Firewall:** Palo Alto, FortiGate.
- **Check point OS:** Windows, Linux.

CERTIFICATION

- Certified Ethical Hacker- CEH



PERSONAL INFORMATION

Full Name: Nithinraj Bunni

Nationality: Indian.

Marital Status: Single.

Languages known: English, Hindi & Telugu.

EDUCATION

- Integrated MBA from Mahatma Gandhi University.

Nithinraj Bunni