Mohit Kumar Dash

SOC Analyst

Phone: +917978709139

Email: dashmohit9819@gmail.com

Profile Summary

- Over 5.6 years of experience in IT and 3.10 years of relevant experience in Cyber Security including expertise in SOC monitoring, analyzing security logs and network traffic to proactively detect and respond to potential breaches in real-time.
- Possess experience in investigating and responding to a wide range of alerts generated by SIEM. Skilled in utilizing industry-leading tools and technologies to strengthen cyber defense strategies.
- Demonstrated ability to collaborate effectively with cross-functional teams to enhance organizational security posture.
- Seeking leverage expertise in SOC operations to contribute to a dynamic cybersecurity team.

Technical Skills

- Proficiency in monitoring SIEM solutions using ArcSight for event correlation and incident response.
- Analyze security alerts, operations, and maintenance of security devices like SIEM, SOAR, EDR, NTA etc.
- Expertise in analyzing logs from Web servers, Operating systems, Applications, Firewalls and network devices.
- Comprehensive knowledge of Vulnerability Scanning and prioritizing remediation.
- Experience in detecting, triaging, and responding to security incidents.
- Familiarity with MITRE ATT&CK Framework and Cyber Kill Chain.

Educational Qualifications

- B. Tech in Mechanical Engineering from BPUT, Rourkela 2015 – 2019
- Higher Secondary(12^{th}) from Fakir Mohan Junior College, Baleshwar 2013 –2015
- Schooling (10^{th}) from U.N. High School, Baleshwar 2013

Certifications

- Certified Ethical Hacker (CEH) – V11
- Siemplify Certified SOAR Analyst (SCSA)
- Network Defense Essentials (NDE)

Knowledge of Tools

- ArcSight SIEM – Open Text
- SOAR – Open Text
- ITSM(Ticketing) – Micro Focus
- NTA – NetScout
- DDI – Trend Micro
- DDAN – Trend Micro
- NIPS – Trend Micro
- Nessus VA – Tenable
- EDR – ESET
- FortiRecon – Threat Intelligence

Professional Experience

- CONSULTANT – MDR

  March 2022 – February 2025
  Organization Name: Aujas Cybersecurity Ltd.
  Mumbai, India

- SECURITY ANALYST L1

  April 2021 – February 2022

  SYSTEM ENGINEER

  September 2019 – March 2021
  Organization Name: Teras Tech Solutions
  Pvt. Ltd., Bangalore, India

Key Responsibilities

- Provide immediate threat response for Security Event Management team at Security Operations Centre (SOC).
- Perform in-depth investigation of alerts and raise incidents to close alerts as applicable.
- Real time monitoring of Network Security components and devices such as Firewall, Routers, System Application, Windows devices, UNIX devices, Web servers.
- Manage 24x7 operations at SOC, including event monitoring which includes incident detection, tracking and analyzing on a real time basis, report generation.

- Aggregating and Correlating the Logs and Configuring Reports, Queries, Rules, Filters, Dashboards.
- Prepare Log monitoring reports on a daily, weekly, and monthly basis to maintain strict SLA adherence.
- Work closely with Incident Response teams to validate use case effectiveness during real-world incidents.
- Developed and implemented SIEM use cases to detect anomalous activities, enhancing threat detection capabilities and mapped SIEM use cases to MITRE methods.
- Conducted root cause analysis of phishing incidents, documenting findings for reporting and prevention strategies.
- Perform Vulnerability Assessments Scanning using "Nessus" to identify security issues in networks, systems, and applications.
- Created SOAR playbooks for automated and manual blocking of rogue IPs at the firewall level.
- Doing Health-Check of different security solutions on a daily basis.
- Preparation of daily and monthly Threat Intelligence Advisory Reports.
- Demonstrating basic understanding of the MITRE ATT&CK framework to identify adversarial tactics and techniques.
- Escalate issues as per the escalation matrix to the operation heads or senior authorities for faster and better resolution.
- Shift Handover preparation and participating in shift huddle calls & handing over updates to next shift.

Personal Profile

- Name: Mohit Kumar Dash
- Date Of Birth: 01.06.1998
- Gender: Male
- Languages: English, Hindi, Odia

Declaration

I solemnly declare that the items furnished above are true and correct to the best of my knowledge.

Mohit Kumar Dash