KISHORE TN

Chickballapur, Karnataka • +91 7406307139 • Kishorekumartn363@gmail.com
https://www.linkedin.com

PROFESSIONAL SUMMARY

A skilled SOC Analyst with more than 3 years of experience in cloud security tools, including Microsoft Sentinel, Splunk, Defender, EDR, and Sophos. Proficient in phishing email analysis, real-time investigations, and utilizing SIEM tools. Possesses a solid understanding of SOC operations, including monitoring, analysis, incident reporting, and client communications.

SKILLS

- SIEM: Azure Sentinel, Spunk
- Email Security: O365
- Endpoint Security: Microsoft 365 Defender, CrowdStrike Falcon EDR, Sophos EDR, SentinelOne EDR
- Incident Management & Response: ServiceNow, MSP-Manage Engine
- Patch Management: Manage Engine ServiceNow
- Additional Skills: KQL and SPL Queries, Analytics Rules Development, Threat Analysis, Incident Response, Report Preparation, Intrusion Detection and Prevention, Malware Analysis, Log Management, Phishing Email Analysis, Firewall and IDS/IPS Management

WORK EXPERIENCE

SOC Analyst L1
Rezilyens System Software Pvt Ltd, Coimbatore
March 2022 - August 2024

- Monitor and analyze SIEM alerts using various security tools.
- Develop analytics rules, incidents, playbooks, workbooks, and KQL queries for data normalization in Log Analytics.
- Conduct endpoint analysis and remediation activities using Defender.
- Investigate and close false positives, and raise tickets for validated incidents.
- Analyze phishing emails, domains, and IPs, recommending appropriate blocking actions.
- Prepare daily, weekly, and monthly incident reports.
- Use escalation processes for multi-user impacting incidents, keeping management updated on progress.
- Proficient in incident response processes including detection, triage, incident analysis, remediation, and reporting.
- Analyze malicious links and executables in sandbox environments to understand their behavior.

Cyber Security Analyst
Zalaris HR Services India Pvt Ltd
September 2024 - Present

- Monitor and analyze SIEM alerts using Splunk and other security tools.
- Create correlation rules, playbooks, and SPL queries for event correlation and data normalization.
- Analyze phishing emails, domains, and IPs, recommending appropriate blocking actions.
- Prepare daily, weekly, and monthly incident reports within Splunk.
- Evaluate and implement SIEM use cases.
- Deep packet analysis, Collection of IOC (Indicator of Compromise), Collection of Evidence.
- Identify vulnerabilities and recommend corrective measures to patch.
- Proficient in incident response processes, including detection, triage, incident analysis, remediation, and reporting in Splunk

EDUCATION

Bachelor of Engineering
University BDT College of Engineering, Davanagere
- August 2015 - August 2019

CERTIFICATIONS

- Certified SOC Analyst Foundation
- SC-200 Microsoft Security Operations Analyst

TOOLS AND TECHNOLOGIES

- SIEM: Azure Sentinel, Splunk
- Email Security: O365
- Endpoint Security: Microsoft 365 Defender, CrowdStrike Falcon EDR, Sophos EDR, SentinelOne EDR
- Incident Management & Response: ServiceNow, MSP-Manage Engine
- Patch Management: Manage Engine pro