ANOOP KALAMNURIKAR

Pune, India 411045 • 8605640281 • kalamnurikaranoop@gmail.com

PROFESSIONAL SUMMARY

I have overall 4+ years of experience in IT as a Security Researcher and Analyst. I would love to work in a company where I can utilize my skills and improve my career path.

Specialized in proactive network monitoring of SIEM (Splunk)/Azure Sentinel and EDR Carbon Black. Have a deep knowledge of identifying and analyzing suspicious events.

EDUCATION

Bachelor of Engineering : Electronics & Communication Engineering, 10/2010
Swami Ramanand Teerth Marathwada University - Nanded, Maharashtra, India

SKILLS

- Incident response, Detection, and Investigations
- SIEM - Splunk Es, Azure Sentinel
- EDR - Carbon Black & Microsoft 365 Defender.
- Firewall - Cisco ASA, Palo Alto, FortiGate & Cloud Flare WAF.
- Familiarity with security technologies, including firewalls, IDS/IPS, and endpoint protection.
- Knowledgeable about cyber security frameworks, compliance standards, and best practices.
- Security operations | Endpoint Security - McAfee ePO | Symantec
- Open Source Intelligent Tools: VirusTotal. IPvoid, AbuseIP, URLscan, Cisco Talos, URLvoid

WORK HISTORY

SOC Analyst, 04/2022 - Current
NTT Data - Pune, India

- Working in Security Operation Centre (24x7), monitoring SOC events, detecting and preventing intrusion attempts.
- Splunk ES / Azure Sentinel & Carbon Black EDR, Working on monitoring of alerts, analyzing, coordinating with concerned teams with remediation steps and triaging them as True positive and False Positive .
- Monitoring, analyzing, and responding to infrastructure threats and vulnerabilities. Collecting the logs of all the network devices and analyze the logs to find the suspicious activities.
- Monitored and analyzed security events using SIEM tools to identify potential threats and anomalies.
- Perform incident monitoring, response, triage and initiate investigations Create and track incidents and request using ticketing tool: (Service Now).
- Perform Malware Analysis by Static and Dynamic methods to identify the malicious IOCs-indicator of compromise, taking action around IOCs identified.
- Investigate all reported suspicious emails and determine whether the emails are malicious, non-malicious or legitimate and reply to the user who reported the suspicious email with a message reporting the findings and any recommendations.
- Monitoring and perform in-depth analysis of security alerts using the Carbon Black platform.
- Investigated and triaged alerts, ensuring timely response and resolution of security incidents.
- Investigate malicious phishing emails, domains and IPs using Open Source tools and recommend proper blocking based on analysis. Continuously monitoring and interpreting threats using the IDS and SIEM tools.
- Conducted analysis of network traffic, logs, and alerts to identify signs of unauthorized activities.

Cyber Security Analyst, 02/2020 - 03/2022
Hexaware Technology Solutions - Pune, India

- Worked in 24x7 operational support
- Performing real-time Monitoring, Analyzing, and Investigating of logs with Reporting, Escalation and resolve of various Incidents/Events/Security Alerts triggered in SIEM tool from multiple log sources.
- Splunk ES / Azure Sentinel & Carbon Black EDR, Working on monitoring of alerts, analyzing, coordinating with concerned teams with remediation steps and triaging them as True positive and False Positive
- Identify and ingest indicators of compromise (IOCs), e.g malicious • IPs/URLs, e.g., into network tools/applications Stay up to date with current vulnerabilities, attacks.
- Performing real-time Monitoring, Analyzing, and Investigating of logs with Reporting, Escalation and resolve of various Incidents/Events/Security Alerts triggered in SIEM tool from multiple log sources.
- Providing logs to different teams from Splunk ES/Azure Sentinel as and when request for logs received.
- Performing real-time Monitoring, Analyzing, and Investigating of CloudFlare WAF Alerts and Logs.
- Perform Malware Analysis by Static and Dynamic methods to identify the malicious IOCs-indicator of compromise, taking action around IOCs identified.
- Investigate all reported suspicious emails and determine whether the emails are malicious, non-malicious or legitimate and reply to the user who reported the suspicious email with a message reporting the findings and any recommendations.
- Mentored junior analysts, providing training on incident analysis, threat intelligence, and response best practices.
- Contributed to the development of custom correlation rules and signatures to enhance detection capabilities specific to the organization's environment.
- Actively monitored threat intelligence sources to stay informed about the latest attack vectors, vulnerabilities, and emerging threats.
- Worked closely with network and system administrators to implement security controls and configurations that aligned with best practices.

Network Analyst, 04/2017 - 01/2020
FIS Global - Pune, India

- Maintained network hardware and software and monitoring network to support network availability to end users •
- Monitored system performance and responded to alerts
- Installed, configured, and supported local area network (LAN), wide area network (WAN), and Internet system
- Handling TAC Cases for all over APAC/EMEA Region for various Network issues Experience with SIEM, IDS/IPS.
- Coordinated with third-party security information and event management (SIEM) providers to maintain protections and predict threats.
- Maintained data management and storage systems to protect data from compromise.
- An understanding of TCP/IP, VLAN, STP, VTP, HSRP, OSPF, EIGRP, Switch Port Security and have implemented almost of these protocols in the hierarchical networks.

CERTIFICATIONS

- SC- 200 - Microsoft Security Operations Analyst
- CCNP (Routing & Switching) | CCNA, CCNP (Security)

LANGUAGES

English

Hindi

Advanced (C1)

Advanced (C1)

Marathi

Advanced (C1)