AMIT KAPOOR

Mobile: +91 8700312286 and 9643807110 (WhatsApp) Email: amitkapoor.cs@gmail.com

LinkedIn Url: https://www.linkedin.com/in/amit-kapoor-aa27b5238/

Professional Synopsis

Cyber Security Engineer and results-driven professional with 9+ years of progressive experience in Security Operations (SOC), Incident Response (IR), and GRC/IT Audit. Expertise includes leading threat detection/hunting initiatives (MITRE ATT&CK), and performing security control audits against standards like ISO 27001. Seeking a Security Analyst or Security Audit role to leverage technical proficiency and deliver high-fidelity security and compliance results.

Core Competencies

- Security Stack: ArcSight (ESM & Logger), Seceon aiSIEM, Sentinel One & Elastic EDR, Trellix DLP, FortiGate, IDS/IPS, Zscaler (ZIA/ZPA), SOAR automation to reduce MTTR.
- GRC, Audit & Compliance: ISO 27001 (ISMS), Audit Readiness, Control Reviews.
- Threat Analysis & IR: Proactive detection of IOCs/IOAs, APTs, C2 traffic, data exfiltration; RCA and containment strategies aligned to MITRE ATT&CK & Cyber Kill Chain.
- OS & Forensic Analysis: Windows/Linux event monitoring, Log Review and Analysis, Anomaly Detection, Malware Analysis Basics, Packet/Network Flow Analysis.
- Authentication & Access Control: Identity and access management using Okta, SAML, and secure traffic inspection via Zscaler.
- Email Security & Phishing Orchestration: Leveraged knowledge of Email Security Gateways to investigate and mitigate sophisticated spear-phishing, whaling, and BEC campaigns by analyzing mail headers and enforcing SPF, DKIM, and DMARC authentication protocols.

Professional Experience

Skillmine Technologies | June 2025 – August 2025 **Senior Cyber Security Engineer – Full Time**

- Assisted with the security control auditing and internal audit process across enterprise environments, managing evidence collection and control effectiveness documentation to align with NIST CSF functions and compliance standards including ISO 27001.
- Monitored and triaged security alerts using SIEM platform (ArcSight) to detect intrusions, malware activity, and anomalous behaviors across enterprise environments.
- Conducted proactive threat hunting across firewall, Zscaler, WAF, Proxy, and endpoint logs to uncover IOCs, IOAs, APT activities, and anomalies not detected by existing rules.
- Investigated malicious outbound connections (IPs, domains, C2 servers, abnormal ports, website defacements) to identify data exfiltration attempts and command-and-control communication.
- Performed root cause analysis (RCA) and log correlation for high-severity incidents, mapping techniques to the MITRE ATT&CK framework and recommending containment/eradication strategies.
- Integrated Threat Intelligence (TI) feeds, OSINT, and sandbox analysis into investigations, enabling early detection of evolving threats and reducing false negatives.
- Enhanced SIEM use cases, correlation rules, and dashboards, continuously tuning detection logic for higher-fidelity alerts.
- Implemented SOAR automation playbooks for repetitive incident-handling tasks, reducing MTTD/MTTR and improving SOC efficiency.
- Documented threat investigations, playbooks, and lessons learned, ensuring knowledge sharing and repeatable processes within the SOC.
- Monitored network security controls (FortiGate firewall, IDS/IPS, SentinelOne EDR, ensuring compliance with customer security policies and regulatory standards.
- Collaborated with SOC and IR teams to track emerging CVEs, threat campaigns, and attacker TTPs, adjusting hunting strategies and maturing the detection program.

CDAC | June 2024 – February 2025 **Project Engineer – Full Time**

- Contributed to the audit readiness program by assisting in the security control review process, focusing on evidence collection and documentation for checks across IT infrastructure assets. Ensured input aligned with ISO 27001 and compliance standards.
- Managed, monitored firewalls (FortiGate), IDS/IPS, and SIEM solutions like Seceon aiSIEM and Elastic EDR to ensure optimal security posture.
- Collaborated with IT teams for detailed quality assurance reviews of cybersecurity incidents, ensuring accurate documentation, timely resolution, and adherence to organizational standards and industry best practices.
- Performed RCAs, with a primary focus of eliminating the threats to a network and determining the cause of the security incident while preserving evidence/logs for further analysis.
- Provided Onshore security support to the National client(s).
- Optimized SOAR solutions to enhance security automation and incident response efficiency.
- Triage, Review and Implement security specific changes in line with Customer Security Policies and change control processes.
- Carried out in-depth investigation on security events.
- Monitored SIEM and logging for alerts of potential network threats, intrusions, and/or compromises.
- Integrated and shared information with other analysts and teams to proceed for deep investigations.
- Tools: Seceon aiSIEM, FortiGate, ITSM (SDP), Arista CloudVision, Elastic EDR and KIBANA.

BT Group | April 2016 – January 2024 **Security Associate – Full Time**

- Monitored and optimized Splunk ES correlation rules, dashboards, and data models to monitor high-volume environments for intrusions, malware, and anomalous behaviors.
- Managed and tuned Palo Alto Networks firewalls (App-ID, Content-ID), IDS/IPS, and Zscaler/Proxy logs to ensure a robust security posture and perimeter integrity.
- Performed end-to-end incident lifecycles by leveraging EDR monitoring and forensics to detect, contain, and eradicate sophisticated threats while preserving critical evidence and logs.
- Managed custom SOAR automation playbooks for repetitive incident-handling tasks, significantly reducing MTTD/MTTR and improving overall SOC efficiency.
- Conducted hypothesis-based threat hunting across firewall, proxy, and endpoint logs to uncover stealthy IOCs, IOAs, and APT activities missed by existing detection logic.
- Spearheaded deep-dive RCAs and log correlation for high-severity incidents, mapping attacker techniques to the MITRE ATT&CK framework to drive long-term architectural hardening.
- Conducted audit readiness programs by conducting security control reviews and managing evidence collection to ensure 100% alignment with ISO 27001 and NIST CSF standards.
- Integrated TI feeds, OSINT, and sandbox analysis into investigations to enable early detection of evolving threats and track emerging CVEs.
- Led detailed QA reviews of cybersecurity incidents and documented playbooks/lessons learned to ensure knowledge sharing and provide technical mentorship to the SOC team.
- Triaged and implemented security-specific changes in strict accordance with Customer Security Policies and formal change control processes for national-level clients.
- Partnered with IT and Onshore/Offshore teams to track attacker TTPs, providing technical support and adjusting hunting strategies to mature the organizational detection program.
- Investigated malicious outbound connections (C2 servers, abnormal ports, and website defacements) to identify and prevent data exfiltration attempts.
- Monitored network security controls and Elastic EDR to ensure continuous compliance with customer security policies and regulatory standards.

HCL Technologies | June 2015 – January 2016 **Junior Engineer – Full Time**

- Provided technical support and troubleshooting for high-speed broadband and fiber-optic connectivity, ensuring stable network access for enterprise and residential clients.
- Diagnosed and resolved hardware issues involving hubs, routers, and switches, including the configuration of LAN/WAN settings and DHCP/DNS troubleshooting.
- Managed the end-to-end diagnostic process for ONT/ONU devices and residential gateways, verifying signal integrity and light levels for optimal performance.
- Responded to and resolved help desk tickets within established SLAs, documenting all hardware installations, software configurations, and network repairs.
- Collaborated with senior engineers to troubleshoot physical layer faults and perform workstation deployments, ensuring adherence to security and connectivity standards.

Academic Qualification

- MBA (IT) | Kurukshetra University, Kurukshetra, India | 2025 - Pursuing
- B.Tech (ECE) | Kurukshetra University, Kurukshetra, India | 2022
- Diploma in Engineering (ECE) | Maharishi Markandeshwar University, Ambala, India | 2012

Certifications and Trainings

- Description: DIAT Certified Information Assurance Professional
  Organization: Defense Institute of Advanced Technology DIAT (DU) DRDO, Pune
- Description: CCNA (Routing & Switching)
- Fortinet Certified Fundamentals in Cybersecurity
- Netskope Cloud Security Specialist