POOJA KAUSHIK

CYBERSECURITY ANALYST/ENGINEER

Email ID: kaushik.pooja126@gmail.com

Location: Hoboken, New Jersey

Phone No: 201 927 5217

https://www.linkedin.com/in/pooja-kaushik-12785515a/

PROFESSIONAL SUMMARY:

- Cybersecurity Professional with close to 6 yrs. of experience across different security domains including Secure Architecture, Zero Trust, DevSecOps, Cloud Security, Data Security, Network Security, Identity Access Management, Enterprise Risk Management, Risk and Compliance, Threat & Vulnerability Management, Security Operations, Application Protection etc.
- Designing security solutions in line with different risk and regulatory frameworks (i.e., ITIL, ISO 27001/2, NYCRR Part 500, PCI-DSS, HIPAA, GDPR, OWASP, CSA, NIST, etc.).
- Proficient in vulnerability assessment tools like Nessus, Qualys, and Rapid7. Experience in conducting penetration testing and vulnerability scanning.
- Proficient in safeguarding organizations by designing secure cloud architectures, managing risk and compliance, identifying and mitigating threats and vulnerabilities, implementing robust security solutions and leveraging SIEM tools for real-time threat detection.
- Skilled in implementing risk management frameworks and ensuring compliance with industry regulations such as GDPR, HIPAA, and ISO 27001. Familiarity with tools like RSA Archer, ServiceNow GRC, and MetricStream.
- Perform security assessments and threat modeling in cloud environments (AWS, Azure, and GCP) to ensure proactive measures working with the DevOps team.
- Expertise in designing and securing cloud environments using platforms such as AWS, Azure, and Google Cloud. Proficient in tools like AWS Security Hub, Azure Security Center, and Google Cloud Security Command Center.
- Strong knowledge and experience of the latest cloud security trends like cloud-native application protection platform (CNAPP), cloud security posture management (CSPM), cloud workload protection (CWP) and DevOps security.
- Experienced in setting up and managing the process to perform patching for critical security issues and vulnerabilities.
- Strong understanding of IAM principles and experience with tools like Azure Active Directory, CyberArk, Ping Identity, and SailPoint. Proficient in user provisioning, access controls, conditional access, role-based access (RBAC) and multi-factor authentication (MFA).
- Skilled in leveraging SIEM solutions such as Splunk, ArcSight, and LogRhythm for log analysis, threat detection, and incident response. Familiarity with log management tools like ELK Stack (Elasticsearch, Logstash, Kibana).
- Experience working with leading cybersecurity vendors and service providers such as Palo Alto Networks, Cisco, Fortinet, Trend Micro, and Symantec. Collaborates with vendor teams for product evaluations, implementations, and ongoing support.
- Dedicated to staying updated with emerging technologies, industry trends, and evolving threat landscape. Actively participates in training programs, conferences, and industry certifications such as CISSP, CISM, and CCSP.

CERTIFICATIONS:

- CISA (Certified Information Systems Auditor)
- Microsoft Certified Azure Fundamentals (AZ-900)
- AWS Certified Solutions Architect - Associate (SAA-C03)

- FortiGate Network Security Expert (NSE-1)
- FortiGate Network Security Expert (NSE-2)
- FortiGate Network Security Expert (NSE-3)
- Diploma | Google Cybersecurity Professional

TECHNICAL EXPERTISE:

Risk & Compliance: Creation, review and implementation of policies and procedures established with regulatory requirements.

Tools/Technologies/Frameworks: CIS, NIST, OWASP, NYCRR Part 500, Archer, ServiceNow, SAP GRC, ISO27001, PCI-DSS, HIPAA, SOC audits and Risk assessments

Cloud Security: Designing and implementing secure architectures on public, private and hybrid cloud environments (AWS, Azure, and GCP).

Tools/Technologies: Wiz, Prisma, Twistlock, Dome9, Aqua Security, Defender for cloud, Azure NSGs, Azure firewall, Azure Application Gateway, Azure AD, Azure DDoS Protection, Key Vault, Infrastructure as Code (IaC), Azure Sentinel, AWS Config, GuardDuty, Amazon Macie, AWS CloudTrail, Security Hub, AWS Inspector, AWS Shield, AWS WAF, AWS Secret Manger, Security Command Center, Cloud Armor, VPC Service Controls, Cloud Firewall, Cloud IDS, Cloud Key management

Threat & Vulnerability Management: Identifying, classifying, remediating, and mitigating weaknesses in different environments.

Tools/Technologies: Tenable Nessus, Qualys, Rapid7, Tripwire, Tanium, Wireshark, Nmap, IBM X-Force, SCCM, PatchMyPC

Security Operation Center (SOC): Daily operations of monitoring, managing, troubleshooting, and remediating security issues/alarms for the complete IT environment.

Tools/Technologies: Splunk, ArcSight, LogRhythm, SolarWinds, FortiSIEM, Rapid7, Azure Sentinel, Chronicle SOAR, ServiceNow Security Incident Response (SIR)

Network Security: Fortinet, Palo Alto, Checkpoint, Cisco Firewall, Symantec Web Gateways, ZScaler, McAfee IPS/IDS

Data Security: Symantec, Varonis, Microsoft, MacAfee, Thales, IBM, Micro Focus, Imperva

Identity and Access Management (IAM): Receive and process requests for account provisioning, modification, and de-provisioning.

Tools/Technologies: Azure AD, Conditional Access, MFA, RBAC, AWS IAM, Okta, Ping Identity, CyberArk

Other Tools: ServiceNow, Jira, Azure DevOps, MS Visual Studio, JSON, Python, PowerShell, Terraform

PROFESSIONAL EXPERIENCE:

Company: Sumitomo Mitsui Trust Bank, USA
Duration: June 2023 – Present
Location: Hoboken, New Jersey
Information Security/ & IT Risk Analyst

Responsibilities:

- Collaborated closely with auditors, Chief Information Security Officer (CISO), and customers to provide requested information and address inquiries effectively.
- Assisted CISO in Vendor Management tasks, including conducting annual assessments and overseeing necessary follow-ups.
- Supported the annual IT Risk Assessment process, working alongside the CISO and Chief Information Officer (CIO) to assess and mitigate risks.
- Conducted comprehensive annual assessments of the evolving cyber security threat landscape, providing insightful recommendations for proactive measures.
- Developed and tested Cyber Security Event Response procedures to ensure rapid and effective responses to potential incidents.
- Worked collaboratively with the infrastructure team, contributing to production support activities as directed and optimizing operational efficiency.
- Investigated and managed security breaches and cyber security incidents, ensuring timely resolution and minimal impact on operations.
- Documented security breaches comprehensively, assessing the extent of damage caused and identifying areas for improvement.
- Planned, executed, and monitored security measures to safeguard TRA corporate infrastructure and critical information assets.
- Implemented and maintained robust security controls, guaranteeing the integrity, confidentiality, and availability of TRA data and infrastructure.
- Developed, communicated, and updated cyber security policies and procedures, ensuring adherence throughout the organization.
- Conducted thorough compliance monitoring activities, confirming the alignment of policies with corporate guidelines, legal requirements, and regulations.
- Prepared detailed reports based on monitoring findings, including recommended enhancements and remedial actions to address vulnerabilities.
- Deployed and managed specialized software tools in support of strategic Cyber Security initiatives, enhancing overall security posture.

Company: Ogma Consulting Pvt Ltd

Client: Leading Bank in the US (Wells Fargo)

Duration: 2 years 9 Months (Aug,2020 – Arpil,2023)

Cybersecurity Analyst

Responsibilities:

Vulnerability Management & Incident Response:

Worked as a Security Analyst on the Vulnerability Management and Security Operations team.

- Operate and maintain vulnerability scanning tools tailored to the organization's environment, such as Tenable.sc, Qualys Guard, or Rapid7 InsightVM.
- Perform threat modeling for different cloud services (including AWS, Azure, and GCP) in line with STRIDE and other standards methodologies.
- Working with SRE and DevOps team to publish threat models for different CSPs to ensure proactive security measures.
- Manage the process to perform application packaging and patching using industry best practices

and tools.

- Design and configure policies in the different VM tools in line with security standards such as CIS benchmarks.
- Work on Microsoft SSCM and IBM Endpoint Manager to perform patching for Windows, Linux, and other OS endpoint management.
- Collaborate with system administrators, network engineers, and application owners to identify assets, define scanning scopes, and ensure comprehensive coverage.
- Configure and schedule regular vulnerability scans based on organizational requirements and compliance standards (e.g., CIS, PCI DSS, HIPAA, ISO 27001).
- Analyze scan results and generate actionable reports, highlighting critical vulnerabilities, prioritized based on the organization's risk appetite and impact on business operations.
- Work closely with IT teams to track and validate the remediation of identified vulnerabilities within defined SLAs.
- Conduct manual vulnerability assessments, utilizing tools like Burp Suite or Metasploit, to identify potential vulnerabilities missed by automated scans.
- Collaborate with the patch management team to align vulnerability remediation efforts with patching processes and schedules.
- Conduct periodic vulnerability trend analysis to identify recurring issues and propose long-term remediation strategies.
- Coordinate with external vendors and penetration testers to conduct in-depth vulnerability assessments and penetration tests.
- Continuously enhance the vulnerability management program by implementing automation, integrating with ticketing systems (e.g., Jira, ServiceNow), and leveraging threat intelligence feeds.
- Provide technical guidance and training to IT teams and stakeholders on vulnerability management best practices and secure configuration standards.
- Identify manual security processes that can be automated to improve efficiency and reduce human error.
- Collaborate with cross-functional teams to gather requirements and design automated security solutions tailored to the organization's environment.
- Integrate security tools and technologies (e.g., SIEM, IDS/IPS, vulnerability scanners) into automated workflows to enable real-time threat detection and response.
- Create and maintain security playbooks and runbooks to document automated security processes and procedures.
- Conduct periodic audits and assessments of security automation processes to identify areas for improvement and optimization.

Information Security Analyst: Served as a Security Analyst in the client's Security monitoring team to enhance the existing processes and manage ongoing security incidents. The role included
below key responsibilities:

- Performing analysis of security events involving data collected from the network, host systems, and application log data.
- Supporting the development and maintenance of vulnerability management services including vulnerability scanning and tracking support for vulnerability remediation.
- Prioritizing remediation tasks based on risk level, and assigning them to the relevant system owner, and monitor progress until completion
- Applying root cause analysis to identify and assess problems and key drivers of success.
- Helping onboard new systems and enhance the existing process in place to improve the security monitoring process. and to enhance efficiencies.
- Coordinating with customers regarding scanning schedules and scope reviews.
- Performing security analysis and identifying possible vulnerabilities to create a Vulnerability Assessment report detailing identified exposures with severity & suggestions to mitigate such exposures.
- Generating ad hoc metrics and reports as requested, providing insight into the vulnerability management program's effectiveness.

- Managing SIEM (Splunk, ArcSight), IDS/IPS (Snort, Suricata), incident response, threat intelligence, malware analysis, network security, endpoint security, and vulnerability management (Nessus, Qualys, Rapid7), log analysis, security operations tools.
- Assist in incident response activities by developing and implementing automated incident response playbooks.

Company: ProExcel Technologies Pvt Ltd

Client: Leading Financial Organization in the US (TIAA Bank)

Duration: 2 years 2 Months (May,2018 – August,2020)

Information Security Analyst

Cloud Security: Worked as a cybersecurity analyst to help the customer in securing the cloud data and applications. The role included below key responsibilities -

- Performing deep dive security assessment of the client's existing cloud infrastructure and services to identify the gap areas and security issues. Preparing assessment questionnaire templates in line with cloud security industry standards (i.e., CSA, CIS, NIST, OWASP etc.)
- Delivering final reports highlighting the key concerns and issues in the client's existing cloud
- environment with recommendations to improve cloud security postures.
- Designing data security solutions in cloud environments to protect data through the complete lifecycle.
- Managing and analyzing different data security tools including Microsoft Information Protection, Varonis, MacAfee etc.
- Performing data classification and data labeling for sensitive applications and workloads aligned with organization data policies
- Designing cloud security baselines for client's cloud environment and services including AWS and Azure services.
- Working closely with the DevOps team to integrate security baselines in the process to improve security checks and posture.
- Designing, developing, and implementing security tools, standards, and policies for a secure Azure landing zone.
- Enabling native security controls and vulnerability tools from CSPs (such as Azure Defender, Azure RBAC, Conditional Access, Azure Firewall, Key Vault, NSGs, Security Groups, AWS GuardDuty, AWS WAF etc.).
- Monitor and perform configuration changes on security tools i.e., IPS, WAF, DLP, IAM, SIEM etc.
- Ensured compliance with regulatory requirements by implementing Azure Security Center and Azure Policy for robust security and governance.
- Utilized Azure DevOps for automated deployment and infrastructure-as-code practices using Azure Resource Manager templates.
- Develop and implement security automation scripts and workflows using scripting languages (e.g., Python, PowerShell).
- Work closely with IT and DevOps teams to incorporate security controls into the organization's CI/CD pipelines and cloud infrastructure.
- Collaborate with developers and system administrators to implement secure configuration management and compliance checks using configuration management tools (e.g., Ansible, Puppet, Chef).