**Bikash Dhungana**

**(USC)**

**Senior Cyber Security Engineer**

**Email- bikashudaydhungana@gmail.com Nom-**

**Professional Summary:**

* Proficient in Cybersecurity Engineer with over 11 years of in-depth expertise in Security, Threat Management, Incident Response, Risk Assessments, developing, implementing, comprehensive security solutions to protect data, networks, and systems from cyber threats.
* Managed HBSS McAfee ePO, configured HIPS 8.0 policies, verified and created server tasks, monitored events, created and enforced DLP policy, managed Rogue System Detection
* Support deployment of all HBSS point products and updates to include McAfee agent, HIPS, VSE, DLP. Perform HBSS policy tuning, HIPS, IPS tuning, and all related tasks
* Experienced with Proxy and Malware-mitigation (Bluecoat, Radware/ FireEye), threat detection and data leakage protection (Network DLP/Vontu/Symantec, Bluecoat Security Analytics
* Implement, Configure, Maintain, Fine Tune & Troubleshoot Symantec Data Leak Prevention (DLP) Solution.
* Skilled in leveraging a broad technical skill set, including expertise in Information Security, SIEM, and NIST Risk
* Proficient in leveraging SIEMs (Security Information and Event Management) to collect, correlate, and analyze security logs and events from various sources, enabling proactive threat detection and incident response.
* Experience in planning, developing, implementing, monitoring and updating security programs, and advanced technical inf
* Configure, maintain and design network security solutions including firewalls (Checkpoint, Cisco ASA and Fortinet), IDS/IPS (Cisco, Checkpoint and Sourcefire), VPN, ACLs, Web Proxy, etc.
* Experience configuring and deploying modules and products like McAfee EPO, McAfee VSE, Cloud, McAfee HIPS, McAfee Endpoint Encryption, McAfee Network DLP, McAfee DLP Endpoint, McAfee SIEM.
* Hands-on experience on Web Application Firewalls and attack mitigation techniques
* Work closely with clients Information Assurance analysts to oversee the preparation of a comprehensive and executive and Accreditation (C&A) packages for approval of an Authorization to Operate (ATO); generate, review and update System Security Plan (SSP) against NIST and NIST requirements
* Establish a strong GRC (Governance, Risk and Compliance) practice to ensure adherence to best practice, regulatory requirements and ISO 27001
* Perform Risk Assessment, Gap analysis & create Risk Mitigation plan
* Proficient in implementing and adhering to NIST 800-53v5 guidelines and controls.
* Extensive experience in conducting security assessments and audits based on NIST 800-53v5.
* Skilled in developing and maintaining system security plans (SSPs) in accordance with NIST 800-53v5.
* Skilled in identifying and mitigating security risks by applying NIST 800-53v5 controls.

**Southern California Edison (SCE), Rosemead, CA April- 2022 to Present**

**Senior Cyber Security Engineer**

**Responsibilities:**

* Conducted security assessments, protection requirements analysis, and risk analysis for cloud Platforms.
* Strong proficiency in network security, designing Network Access Control Lists (NACLs), Ingress/Egress policies, and implementing DDoS/IPS/IDS measures.
* Working with DLP, Bluecoat web sense, Proofpoint, Trend Micro, and IBM QRadar Enterprise SIEM security tools to monitor network environment.
* Monitored and analyzed security event data through SIEM, identifying and responding to emerging threats and anomalies.
* Implemented automation solutions within the SOC environment, focusing on SOAR capabilities to enhance incident response workflows and playbook execution.
* Participated in Agile project teams, contributing to the successful delivery of IAM initiatives.
* Co-ordinating pen testing and application security testing audits with Pen Test Tools like Metasploit, NMAP, Wireshark and Kali on Linux/Unix operating system.
* Extensive experience in creating and updating documentation (Engineering and Support)
* Configured endpoint device controls using CrowdStrike. Worked on compromised endpoint incidents.
* Monitored CrowdStrike EDR alerts and dashboards for potential threats, analyzing data to identify patterns and anomalies.
* Conducted cross-term IT team security assessments to identify security gaps.
* Produce efficient DLP policies to ensure necessary in/outbound emails are logged.
* Ensuring Symantec DLP policies are in place and scanning the environments for incidents.
* Performed tuning of Symantec DLP to reduce false positives and improve detection rates.
* Integrated CrowdStrike Falcon with SIEM and SOAR (Security Orchestration, Automation, and Response) platforms.
* Design, development, implementation, tuning and testing of standard and nonstandard content for McAfee SIEM (Nitro).
* Implemented and maintained SOX/SOC1/SOC2 controls to ensure compliance across IT operations.
* Managed user access and privileges using Saviynt, automating account provisioning and deprovisioning processes.
* Developed complex SQL queries to extract, analyze, and report on user access data, improving audit accuracy.
* Led Agile development sprints to integrate IAM solutions with existing systems, enhancing security and efficiency.
* Perform Digital forensics and Incident Response (IR) using tools Autopsy, Magnet, Stinger, etc. 28 DOL agencies
* Maintained GIT repositories, branches and tags and Experience in Administering GITHUB repository.
* Played a key role in deploying Symantec Endpoint Protection Manager and clients on a closed network
* Worked as a PCI-DSS consultant to perform a 3rd party audit.
* Built and maintained a security API portal in Python, enabling seamless integration with security tools and systems.
* Monitored and managed security event management systems (SIEM) to detect and respond to security incidents and anomalies.
* Developed and implemented automation scripts and workflows to enhance SOC efficiency, focusing on incident response automation and playbook creation.
* Configured and tuned CrowdStrike policies and rulesets to optimize threat detection and prevention.
* Configured Office 365 Advanced Threat Protection (ATP) for email and file protection against advanced threats.
* Configured Zscaler Cloud Firewall policies to enforce security controls for internet-bound traffic.

**ERICSSON INC- Santa Clara, CA December- 2020 to March 2022**

**Sr. Cybersecurity Engineer**

**Responsibilities:**

* Provided ICS cyber security advice in client engagements (including assessment, design and implementation of security in Linux environments and security infrastructure for IT/OT risk solutions) Provided professional analysis through trusted expertise.
* Expertise in development of Information Security Programs based on frameworks such as NIST, NIST, NIST, ISO 27002, COBIT 5.0, FFIEC, GLBA, SOX, PCI & PII with IT Risk drivers KPI's and KRI's to ensure Financial regulatory compliance and data security.
* Conduct internal and external security audits based on standard cybersecurity frameworks from ISO 27002, COBIT, NIST, OWASP and Cloud Security Alliance
* Involved in DLP data encryption, monitoring/reporting and remediation of internal and external threats/vulnerabilities
* Responsible for identifying and validating indicators of threat from multiple Intel sources (i.e. Crowdstrike, FS-ISAC, Bluecoat, etc.) against internal assets to determine an accurate threat landscape and remediation targets (i.e. Splunk endpoint analysis, Vulnerability analysis (Qualys, Nessus, Metasploit).
* Designing and maintaining production-quality Splunk dashboards.
* Built proof of concept (POC) for Localization to use AWS for some transcoding workloads. AWS services used were EC2, S3, Lambda, Elastic Transcoder. The second phase would be to add Captions and Digital Rights Management (DRM).
* Assessment guidance/standards used; NIST SP, NIST, NIST, ISO27002, ISO27005, to ensure regulatory compliance and proper assessment of risk.
* Develop documentation for new/existing policies and procedures in accordance with the Risk Management Framework (RMF), NIST SP requirements.
* Engineered a security API portal using Python to automate security processes and integrate with various security platforms.
* Configuring rules and Maintaining Palo Alto Firewalls& Analysis of firewall logs using various tools
* Conducted regular audits of SOX/SOC1/SOC2 controls, identifying gaps and recommending improvements.
* Administered IAM tools to manage user roles and permissions, ensuring adherence to compliance policies.
* Utilized Excel to create detailed reports and dashboards, enabling better visibility into access management.
* Collaborated with cross-functional teams in Agile settings to develop and implement IAM-related features.
* Developed executive-level presentations in PowerPoint to communicate cybersecurity strategies and initiatives.
* Created process flowcharts in Visio to illustrate incident response procedures and workflows.
* Used Excel for budget planning and financial analysis related to cybersecurity initiatives and projects.

**CON EDISON – NY Feb 2018 to October 2020**

**Cyber Security Engineer**

**Responsibilities:**

* Coordinate and conduct event collection, log management, event management, compliances automation, and identity monitoring activities using SIEM platform.
* Provide IT Governance, Risk, and Compliance (GRC) service to fulfil client requirements
* Developing in-house automation projects in Python, PowerShell for the consumption of SOC.
* Prepared vulnerability compliance, operating system security compliance and MDM compliance reports.
* Conducted weekly KCI’s (Key Control Indicator) review calls with senior management to prioritize remediation.
* Assess vulnerabilities identified in Qualys and communicate with product / services owners for remediation.
* Provided expert guidance on SOX/SOC1/SOC2 compliance, helping clients align their IAM practices with regulatory standards.
* Assisted in the deployment of IAM tools, including Saviynt, to streamline access management processes.
* Perform analysis and triage on activities and incidents within the data protection environment including, but not limited to Digital Guardian DLP
* Involved in Digital Guardian DLP data encryption, monitoring/reporting and remediation of internal and external threats/vulnerabilities SME (Subject matter expert) on SIEM and writing detection rules on the platform Scripting or programming experience in Python and PowerShell.
* Managed Cyber Security threats through prevention, detection, response, escalation and reporting in effort to protect Enterprise IT Assets through Computer Security Incident Response Team (CSIRT)
* Proactively implemented updates, maintained, managed, monitored, and supported enterprise network and systems security operations infrastructure throughout the shared services environment.
* Responsible for delivering an end-to-end continuous integration - continuous delivery system for the products in an agile development approach using Chef/Ansible and Jenkins and Shell Scripts.
* Wrote Ansible playbooks to set up Continuous Delivery pipeline and this primarily consists of a Jenkins and Sonar server, the infrastructure to run these packages and various supporting software components such as Maven.
* Managed the large security, risk and compliance initiatives of SOX-404 IT, PCI DSS and HIPAA/HITECH, Privacy Act, and FTC including security policies, procedures and controls.
* Experience with Windows, Linux, vulnerability assessment tools, firewalls, IDS/IPS, HIPS/HIDS, Nessus, NMAP, SIEM, Splunk, Rapid7 Nexpose and WAF, routers, switches, VMware, Endpoint Security, Cloud Security, Symantec Endpoint Protection.
* Assesses a residual risk rating for the vendor based upon their control environment
* Monitored SIEM systems for security events, utilizing advanced analytics to detect and mitigate potential threats in real-time.
* Automated routine SOC tasks using Python, including incident response and log analysis, to improve operational efficiency.
* Work with the network team to architecture Azure and AWS VPN, AWS Direct Connect, and Azure Express Route connections
* Analysis and documentation of network & information security requirements and define security policy for enterprise client and business critical servers.

**Honeywell, Charlotte, North Carolina November 2014 to Jan 2018**

**Security Analyst**

**Responsibilities:**

* Implemented physical and procedural safeguards for information resources within the facility. Communicate effectively with senior management, peers, staff, and customers both inside and outside the corporation.
* Administered access to information resources and makes provisions for timely detection, reporting, and analysis of actual and attempted unauthorized access to information resources.
* Monitor client SIEM devices (Splunk) for potential security events that could compromise the client's environment.
* Worked along with the Windows System Administrator for securing the Windows Environment.
* Coordinated efforts with DLP engineering and escalations to cyber investigations
* Crafted SQL queries for in-depth data analysis, supporting audit and compliance efforts.
* Created a Python-driven security API portal to centralize security tool management and enhance data sharing across the security ecosystem.
* Implemented and fine-tuned SIEM systems to continuously monitor security incidents, ensuring timely detection and response.
* Developed custom automation scripts for SOC operations, leveraging SOAR to optimize incident response and threat mitigation processes.
* Checked all the storage services in Microsoft Azure for all data centers across various locations.
* Monitored and analyzed SIEM events to identify trends and potential vulnerabilities.
* Used Jira for creating defects/blockers in and uploaded evidence in SharePoint.
* Performed audits of IT systems and controls to ensure compliance with SOX/SOC1/SOC2 requirements.
* Assisted in the implementation of IAM tools, focusing on role-based access control and privilege management.
* Developed and maintained SQL queries to monitor and report on access control activities.
* Utilized Excel to analyze audit data and prepare reports for management review.
* Secured configurations of all server images in converge cloud and ensured secure KMS (Key Vault Configuration).
* Created a detailed Incident Report (IR) and contributed to lessons learned and mitigations for future attacks of a similar nature.

**Education Details**

**Bachelor’s in computer science, Nepal, 2013**