Administrator Administrator Administrator - SIEM Tampa, FL Over 7+ years of experience, in field of SIEM Information Security with expertise in Implementation and Operation phasesof the project. Worked in a 24x7 Security Operations Center(SOC). Experience on a Computer Incident Response Team (CIRT), Computer Emergency Response Team (CERT), Computer Security Incident Response Center (CSIRC) or a Security Operations Center (SOC) Provision of guidance and supervision in the de-confliction of critical events while performing incident management coordination during allevents, ensuring that appropriate task teams are actively engaged and maximizing efforts towards restoration and resolution in accordance with organizational SLA's, ITIL Standards Knowledge in Intrusion Detection & Prevention (IDS / IPS), Data Loss Prevention (DLP) analysis tools. Assist with the development of processes and procedures to improve incident response times, analysis of incident, and overall SOC functions Provide Incident Response (IR) support when threat and vulnerability analysis require action Real Time Log monitoring in the Security Operations Centre from different devices such as Firewalls, IDS, IPS, Operating Systems like Windows, UNIX, Proxy Servers, Windows Servers, System Application, Databases, Web Servers and Networking Devices. Responsible for monitoring networks and security tools to detect suspicious and hostile activity across the Environment. Supported for Security Operations Center (SOC). Monitor security system ensure no interruption of service. Identify potential threat, anomalies, and infections and provide report to the customers Monitoring network traffic for security events and perform triage analysis to identify security incidents. Knowledge on QRadar Vulnerability manager and Threat Manager Analyze Threat Patterns on various security devices and Validation of False/True positive Security Incidents. Responding to computer security incidents by collecting, analyzing, providing details evidence (network log files) and ensure that incidents are recorded and tracked in accordance with its guideline and requirements. Knowledge in Authentication, End Point Security, Internet Policy Enforcement, Firewalls, Database Activity Monitoring (DAM), Data Loss Prevention (DLP), Identity and Access Management (IAM) solutions Hands on experience with Change Management working on the incidents and Change Request and coordinating with the APP teams during the cutovers. Provide Incident Response (IR) support

when analysis confirms actionable incident Provide threat and vulnerability analysis as well as security advisory services Analyze and respond to previously undisclosed software and hardware vulnerabilities Ensuring SLA adherence; follow up with the asset owners and ensure that the call raised is closed on time. Develop Operational processes and procedures to appropriately analyze, escalate, and assist in remediation of critical information security incidents. Working on Incident and problem management for resolving incidents within the SLA using ticketing tool like Service Now and JIRA Authorized to work in the US for any employer Work Experience Administrator SIEM - Cisco, NC January 2018 to Present Worked as part of a growing team, in a 24/7 security monitoring SOC Creating Dashboards, Visualizations, Statistical reports, scheduled searches, alerts and worked on creating different other knowledge objects. Document, track and escalate cyber security incidents Monitor and analyze network traffic, Intrusion Detection Systems (IDS), security events and logs. Perform incident response to investigate and resolve computer security incidents Triage intrusionsand other cyber security incidents. Provide Incident Response (IR) support when threat and vulnerability analysis require action Responsible for monitoring networks and security tools to detect suspicious and hostile activity across the environment Monitoring network traffic for security events and perform triage analysis to identify security incidents. Monitor and analyze network traffic and alerts Collaborated with various departments on major security incidents Identitfy potential threats with use of various SIEM tools Created, closed, and made change requests through ServiceNow Working with administrators to ensure splunk is actively and accurately running and monitoring on the current infrastructure implementation Prioritize and differentiating between potential intrusion attempts and false alarms Monitor systems and report the status to client staff on SIEM tool splunk Create daily, monthly and adhoc reports for various devices Knowledge in Intrusion Detection & Prevention (IDS / IPS) tuning, Data Loss Prevention (DLP) Analyze Threat Patterns on various security devices and Validation of False/True positive Security Incidents. Identifying potential threat, anomalies, and infections. Working on Incident and problem management for resolving incidents within the SLA using ticketing tool like Service Now, Remedy and JIRA as well as with Emails. Generates end of shift reports for

documentation and knowledge transfer to subsequent analyst on duty. SOC Analyst CNBC NJ January 2017 to December 2017 Responsibilities: Responsible for working in a 24x7 Security Operation Center (SOC) environment. Maintain meticulous records of security monitoring and incident response activities Monitoring tools and alerts from Security Information and Event Management (SIEM) solutions Monitor and analyze Intrusion Detection Systems (IDS) to identify security issues for remediation Identifies security risks, threats and vulnerabilities of networks, systems, applications and modern technology initiatives Provides technical support in the development, testing and operation of firewalls, intrusion detection systems, and enterprise anti-virus and software deployment tools Integration of IDS/IPS to ArcSight and analyze the logs to filter out False positives and add False negatives into IDS/IPS rule set. Knowledge in Authentication, EndPoint Security, Internet Policy Enforcement, Firewalls, Database Activity Monitoring (DAM), Data Loss Prevention (DLP), Identity and Access Management (IAM) solutions. Hands on experience with Change Management working on the incidents and Change Request and coordinating with the APP teams during the cutovers. Ensure the SOC analyst team is providing excellent customer service and support Notify system administrators and system points of contacts of vulnerability and patch alerts pertaining to their system Provide telephone, e-mail and ticket service to customers Experience in handling clients reported cyber-attacks and incidents. Create, manage and dispatch incident tickets Monitor network and system performances via monitoring tools Respond to security incident tickets and escalate when necessary Provides technical writing for operational documentation SLA analysis and monthly/weekly report preparation. Security Analyst AIG - Fort Worth, TX February 2013 to April 2014 Responsibilities: Worked in a 24x7 Network Operations Center (NOC). Responds to Information Security incidents working in a 24X7 operations department. Experienced in Operations Center environment/team such as: Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT) Monitor and analyze Security Information and Event Management SIEM to identify security issues for remediation. Using internal security tools, perform monitoring and analysis of security events of interest to detect security risks and threats on the customer's network Knowledge in

Intrusion Detection & Prevention (IDS / IPS), Data Loss Prevention (DLP) As a part of Security Engineering team responsible for managing, maintaining and monitoring of Checkpoint firewall. Provides support for operational security tools and technologies by responding to alerts and troubleshooting issues Assist with the development of processes and procedures to improve incident response times, analysis of incident, and overall SOC functions Provide Incident Response (IR) support when threat and vulnerability analysis require action Responsible for monitoring networks and security tools to detect suspicious and hostile activity across the environment. Supported for Security Operations Center (SOC). Monitor security system and diagnoses malware events to ensure no interruption of service. Identify potential threat, anomalies, and infections and provide report to the customers Monitoring network traffic for security events and perform triage analysis to identify security incidents. Analyze Threat Patterns on various security devices and Validation of False/True positive Security Incidents. Identifying potential threat, anomalies, and infections. Researched and tested new security tools/products and make recommendations of tools to be implemented in the SOC environment. Hands on experience with Change Management working on the incidents and Change Request and coordinating with the APP teams during the cutovers. Provide Incident Response (IR) support when analysis confirms actionable incident Provide threat and vulnerability analysis as well as security advisory services Analyze and respond to previously undisclosed software and hardware vulnerabilities Ensuring SLA adherence; follow up with the asset owners and ensure that the call raised is closed on time. Develop Operational processes and procedures to appropriately analyze, escalate, and assist in remediation of critical information security incidents. Working on Incident and problem management for resolving incidents within the SLA using ticketing tool like Service Now and JIRA IT Security Analyst Walmart - Bentonville, AR April 2012 to January 2013 Experienced in Operations Center environment/team such as: Computer Emergency Response Team (CERT), Computer Incident Response Team (CIRT) Provide 24x7 operational support; on a rotating/static shift schedule (including overnight shifts) Experienced in FireEye including analyzing output incidents, and malware reports to devise new and creative ways of detecting and stopping future incidents

Using internal security tools, perform monitoring and analysis of security events of interest to detect security risks and threats on the customer's network Managed Qualys vulnerability scanner to assess risk and provide solutions Monitored incoming event queues for potential security incidents using security management tool Maintain meticulous records of security monitoring and incident response activities Monitor and analyze Intrusion Detection Systems (IDS) to identify security issues for remediation. Responsible for maintaining the integrity and security of enterprise-wide cyber systems and networks. Supported cyber security initiatives through both predictive and reactive analysis, articulating emerging trends to leadership and staff. Generated, obtains, and analyzes security logs and escalate issues to management as appropriate. Using Remedy ticket system to monitored incidents management process and problem management applications with other service management solutions (change, asset, service level, service request, identity, and knowledge). IDS event monitoring and analysis, security incident handling, incident reporting, and threat analysis Monitor and analyze Security Information and Event Management SIEM to identify security issues for remediation. Perform Computer Security Incident Response activities, record and report incidents. Manage the Enterprise Log Management for all critical systems and applications. Prepare briefings and reports of analysis methodology and results System Administrator Zurich Financial Services(ZFS) - Hyderabad, Telangana April 2009 to March 2012 ROLES & RESPONSIBILITIES Managing and maintaining Windows NT,2000,2003, 2008 and 2012 server administration Remote Administration using Terminal Services. Performed Windows user administration, managing user accounts, permissions, User rights, Account policies, Security policies and performed software and hardware maintenance Hands on experience on Remedy7.2, AF Remote, HP Open view, TEPS, HP insight manager, IBM Director, etc. Primary troubleshooting and knowledge in Windows clusters Monitoring & managing Weekly server reboots Performing Disk cleanups and disk management for windows OS drives Working on high CPU and Paging file issues Performing daily checks to ensure stability in the environment Experience in fixing IBM (RSA) and HP (ILO) connectivity with Blade and Brick Servers Working on file/folder restoration issues on user's requests Hands on experience in network devices like

port resets, logs collections, investigations, etc. Working on Incident and problem management for resolving incidents within the SLA using ticketing tool Remedy 7.2 Worked on Service now ticketing tool for creating tickets and changes according to the business requirements. Ensuring that the change process is followed for any configuration changes in the environment. and upon request for technical solutions Physical and virtual Server Rebuilds and Decommissions with proper documentation Responsible for server weekly scheduled reboots and patching schedules on Blade logic and WSUS Worked DR test and was successful in recovering two of client's most critical applications Managing ESX, ESXI hosts and VMs through VMware vSphere server Good knowledge in Installing, Configuring and Managing VMware vSphere. Troubleshooting virtual machine issues like, RDP issues to VMs, Restarting VMs, Application Issues, etc. Monitoring and managing performance of ESX servers and Virtual Machines VMware tools and virtual hardware upgradations Managing snapshots and restoring snapshots of VM'S Working on P2V migrations & V Motion Active participation in SRT for resolving issues with high severity Working knowledge on IBM Blades HS 20/HS 21 /X3650 and ProLiant DL and ML series server hardware platform Firmware & BIOS up gradations. Knowledge on Hardware RAID configurations (RAID 1, RAID 5 ) Basic knowledge on SAN/NAS/DAS environment Creating Normal /Expedited / Emergency CR's according to the business requirement. Education Master's Skills BSD (Less than 1 year), C (Less than 1 year), Checkpoint (1 year), Qualys (Less than 1 year), security (6 years) Additional Information Operating Systems Windows 2000, XP, Win 10, Windows Server, Unix/Linux (Red Hat), Free BSD Security / Vulnerability Tools Snort, Wireshark, Websense, Bluecoat, Palo Alto, Checkpoint Symantec,Qualys Vulnerability Manager, FireEye HX, Sophos, Sourcefire,Nessus,CheckPoint RDBMS Oracle 11g/10g/9i/8i, MS-SQL Server 2000/2005/2008, Sybase, DB2 MS Access, Mysql Networking Protocols and Tools TCP/IP, HTTP/HTTPS, SSH, SSL, DNS, SNMP Routers, Switches, Load Balancers, Cisco VPN, MS- Direct Access, Programming Language C, C++, Java with Big Data, Python, UNIX shell scripts,Javascript Monitoring Tool Netcool,Dynatrace,tealeaf

Name: Kaitlin Wall

Email: nmiller@example.net

Phone: 338-423-1426x93799