Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - Rackspace Tampa, FL, FL Work Experience Senior IT Security Analyst Rackspace - Dallas, TX October 2015 to Present Working in Security Incident and Event Monitoring SIEM platform - IBM Qradar. Security Incident raises according to the alerts and follow-up. Monitoring various event sources for possible intrusion and determine the severity of threat. Experience in IBM Qradar SIEM Integration. Experience in integrating the log sources with IBM Qradar. Creating Reports based on log sources integrated with Qradar for the Customer requirement. SOD Controls and Procedures as a part of Audit Perspective. Technical representation for PCI, CPM and SOX Audit Review and monitoring Experience in SIEM devices health monitoring and capacity management. Experience in Handling and closing high business impact incidents. Experienced in SIEM Technology and analyzing the various Devices Logs. Performing investigation, analysis, reporting and escalations of security events from multiple sources including events like intrusion detection, Firewall logs, Proxy Logs, Web servers. Implementation and Integration of Servers (Windows, Linux and Unix), Security devices like Firewall, IPS, IDS, WAF, Nessus, McAfee Proxy, Symantec Endpoint Protection) Assist with the development of processes and procedures to improve incident response times, analysis of incidents, and overall SOC functions. Experience in Information Security Platform by providing support on known/ unknown vulnerabilities/ threats found via security devices/ product. Experience in developing & creating SIEM Procedures (SOP) documentation. Experience in developing & Fine-tuning SIEM rule alerts and reports. Experience in handling clients reported cyber-attacks and incidents. Network Security (IDS/IPS, N/W Sniffing, Wireshark, TCPDUMP, NMAP). Running vulnerability & compliance scan and report vulnerabilities mitigate risks associated with vulnerabilities reported. Report/Track the vulnerability reports periodically and submit the report to management. Collaborate with worldwide Team members/customers, attend team meetings. Plan, implement and manage vulnerability scanner environment. Interface with vendors to resolve vulnerability scanner related issues and upgrades. Act as subject matter expert and answer questions related to vulnerability scanner. Engage and network with groups outside of IT Services such as Audit Services, Legal, TI businesses, vendors, customers, and partners.

Monitoring Snort (writing rules, monitoring BASE), creating the CASE of unknown alerts, Splunk, Arcsight Writing Snort Signatures, Tripwire (HIDS), and OSSEC (HIDS), Vulnerability assessment using NESSUS. Working on Backtrack UNIX. Shell Scripting. Application/Web Security (OWASP). Audit & Compliance (ISO27001). Wireshark, TCPdump, Ettercap, Cain & Abel, Ettercap, C|EH Modules. IT Security Analyst Ameriprise Financials - Detroit, MI January 2014 to September 2015 working in Security Incident and Event Monitoring SIEM platform - RSA Envision. Security Incident raises according to the alerts and follow-up. Monitoring various event sources for possible intrusion and determine the severity of threat. Hauling Ad hoc report for various event sources and, customized reports, and scheduled reports as per requirements. Collecting the logs of all the network devices and analyze the logs to find the suspicious activities. Monitor RSA envision dashboards to keep track of real time security events, health of SIEM devices.

Investigate the security logs, mitigation strategies and Responsible for preparing Generic Security incident report. Hands on Experience with RSA envision centralized IPDB. Analyze the Malware through static and Dynamic analysis with tools. Responsible to preparing the Root cause analysis reports based on the analysis. Knowledge in Websense, NIPS, Symantec Antivirus, Checkpoint, Active Directory, Cisco switch & Cisco AC Preparation of documents of all aspects of related efforts on intrusion analysis, which is submitted to higher officials to conduct audit and worked with various IT and business unit leads to ensure timely and accurate reports. Responsible for monitoring & acquiring data feeds from a variety of technologies for Splunk (Firewalls, BlueCoat proxy, Windows, Linux, Imperva, RSA, etc) Setup Integration of FireEye alert in other security systems. Setup Automation of FireEye alerts to block infected devices in other security systems. Secured company internet access using BlueCoat proxies. Engineered BlueCoat policies to follow company's policy's & procedures. Responsible for maintaining McAfee IDS/IPS policies. Constructed actionable reports & alerts from RSA Security Analytics. Created & maintained policies for Axway Mailgate & secure email appliances Conducted network vulnerability assessments to identify system vulnerabilities. Developed remediation plans & security procedures Created custom scripts to save time & labor cost on attestation of 50,000 + accounts

Collaborated with other departments in investigations for HiPPA & PCI violations Provide consultative services at the time of PCI audits & reviews. Installed and configured Symantec Enterprise Anti-Virus. Administered and managed SEP Client deployments to Workstations and Servers. Set up policies for servers with specific policies for apps running on servers. Performing DLP inventory scans. Created DLP role-based access controls, DLP device policies, DLP application file access protection. Worked with Global Security Team. Tripwire IP360, Tripwire CCM, Symantec CCS, Nessus, Nmap, Tcpdump, Wireshark, Kali Linux, ArcSight, Splunk. Working with global security team for the Server Compliance and risk management. Working on Symantec ESM (Enterprise Security Manager), Algosec, Tripwire. Working on Mcafee ePO, Mcafee virus scan, monitoring malware activities in the network. IT Security Analyst World Bank February 2011 to December 2013 Implemented SNMP-based networking monitoring tool CACTI, Creating Graphs, Templates, adding CAMM for TRAP Configuration, Setting Threshold. Implemented BACULA as a backup server and Scheduling backup jobs. Working on Puppet (Master & agent) for Monitoring, Reporting & Troubleshooting. UNIX/Linux Administration & Security. Installing and managing virtual machines in Esxi5 (VMWARE), VMotion, SVMotion, DRS, HA, VMware Cloning, Snapshot, creating templates, and Citrix Xen Server. Comprehensive operational knowledge of all major technology areas comprising of virtual & cloud infrastructure. Windows Administration (2003, 2008), Active Directory, DNS, DHCP. IT security intern November 2009 to January 2011 Worked on Multiple Operating Systems Environments likes Windows (2003, 2008) and Linux (Redhat, fedora, Debian), Virtual Infrastructure. Foot printing, Scanning, Sniffing and monitoring Network activities by using Open source & commercial tools like (Wireshark, Nmap).

Conducting cyber forensics activities to check the process of cyber forensics after cyber-crime was conducted successfully by collecting evidence and securing the evidence. Conduct penetration testing & Auditing of the organization network by using tools. Ensure the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices. Use Vulnerability Assessment tool like Nessus to perform security testing Identified new malware infections and removed those remotely

using admin tools or by identifying the user and guiding them through a removal process. Daily research of existing and new security vulnerabilities including 0-day vulnerabilities. Manage users in Active Directory, create mailbox in exchange and assign folder permissions. Research new and evolving threats and vulnerabilities with potential to impact the monitored environment. Make enterprise security recommendations and technical evaluation of new solutions Monitor, evaluate, and assist with the maintenance of assigned security systems in accordance with industry best practices to safe guard internal information systems. Education B-Tech Jawaharlal Nehru Technological University in Computer Science Engineering - Hyderabad, Telangana 2005 to 2009

Name: Katelyn Johns

Email: hdixon@example.net

Phone: 613.795.4928