IT Security Analyst IT Security Analyst IT Security Analyst Atlanta, GA CISSP certified professional with over 6 years of experience in field of Information Security and Networks. Experience in Healthcare, Higher-Ed, Manufacturing and IT industries. I strive to apply my knowledge in broad areas of Information Security and Networks to prepare a holistic solution. I am passionate about Information Security which drives my desire and commitment to continuous skills upgrade. Good at crafting a balanced solution that meet the actual requirement, something that can be put to work and can be updated constantly to meet changing requirements. Ability to initiate and work on project with little or no guidance. Skilled in integrating individual products to create a Multi-layered security solution. Persuading, Influencing and Negotiating Skills. Work Experience IT Security Analyst USAA - Atlanta, GA August 2016 to Present Key Responsibilities ? Monitor security event data from various systems and update incidents accordingly. ? Analyze security incidents and perform forensic analysis for systems and network devices.. ? Monitor for emerging threat patterns and vulnerabilities. ? Run vulnerabilityscans and policycompliance using Qualys ? Generate compliance, remediation reports and track their progress. ? Develop scripts to automate data / log collection. ? Monitor and review Data Loss Prevention incidents and generate reports ? Monitor proofpoint incidents for phishing and malware ? Document configuration and process updates to Wiki IT Security / SOC Analyst NYU Langone Medical Center - New York, NY March 2015 to August 2016 Key Responsibilities ? Review and analyze large sets of security event data to identifytrends and anomalies indicative of malicious activity. ? Perform basic to moderate statisticalanalysis of securityeventdata to identifybaselines, trends, and commonalities. Produce periodic reports on such analysis. ? Research, develop, and keep abreast of tools, techniques, and processimprovements in support of securitydetection and analysis in accordance with current and emergingthreat and attackvectors. ? Maintain / Update SOC, SIEM, MSS, Endpoint protection, DataLossPrevention (DLP) and other security tool correlation / IOC rules. ? Run Vulnerabilityscans, Penetrationtests, and other securityassessments ? Provide Vulnerability / Threatremediationreports and track their progress ? Monitor, administer, and resolve DataLossPrevention tool / incidents. ? Use Security / Forensic tools to monitor, detect, analyze and remediateemail, network, server, and endpoints including medicalequipment. ? Configure, lockdown, and monitorEOL / Critical servers. SOC Analyst Information Security - Chelmsford, MA June 2014 to March 2015 Key Responsibilities ? Monitor, detect, respond, investigate, restore and documentsecurityincidents in cloud environment. ? Work with Dell Secure Works and other teams to resolve Cloud security incidents. ? Maintain Public Key Infrastructure. ? Maintain Active Directory, RADIUS, AAA in cloud environment. ? Designed AAA solution to enhance security and compliance. ? Add / modify security policies on Juniper SRX Gateway and Palo Alto Application firewalls ? Logs monitoring, auditing and reporting using IBM QRadar and Splunk ? Automated backups, polling, monitoring, alerting, SNMP using SolarWinds ? Member / Contributor - Business Continuity team. ? Vulnerability scans using Rapid7 ? Responsible for firewall rules Auditing. ? Patching and upgrading network equipment to remediate vulnerabilities. ? Provide risk analysis inputs to Change Authorization Board ? Assist auditors and other Security teams with SOC compliance checks. ? Application inspection using Palo Alto Firewalls and IDS monitoring using Juniper SRX ? Maintain SilverPeak Wan Accelerator and Load balancing using F5 LTM Security Engineer HCL Technologies / Cisco Systems - Chennai, Tamil Nadu June 2010 to July 2012 Key Responsibilities ? Responsible for IP routing using BGP, OSPF, static routers and switching using STP/VTP Ether-Channel, HSRP, GLBP on Cisco Nexus, Catalyst, ISR, ASR, and Juniper EX series switches. ? Respond to Network, and Serversecurityincidents. ? Maintenance of VMware ESXi and Kernel Virtual Machine (KVM) environment. ? Application load balancing using Cisco ACE. ? Establishing and configuring Site-Site and SSL VPNs on Cisco Firewalls. ? Deployment and maintenance of Certificate Authority. ? AAA services using Cisco ACS. ? Monitoring and reporting using Cisco DCNM, Cisco LAN Management Solution. ? Anomaly detection using Cisco IPS. ? WAN optimization using Cisco WAAS. ? Traffic analysis using Wireshark, TripwireSIEM ? Data analytics using Splunk. ? Failover, HA and data backup configuration on Firewalls, Routers and Switches ? Audited systems generated reports for Compliance ? Responsible for User rights and permissions. ? Disaster recovery planning and validation. Network Administrator Info Aspire Software Solutions - Hyderabad, Andhra Pradesh May 2008 to June 2010 Key Responsibilities ? Deploying the switching functions like VLANS, VTP, STP, and Ether Channel. ? Involved in configuring various protocols like EIGRP, OSPF, etc. for inter-site and intra-site connectivity. ? Establish and maintain Site - Site VPN, and SSL VPN connectivity. ? Reviews project activities for compliance with procedures and standards. ? Securing network devices. ? Responsible for user rights and controls. ? Installing operating systems on user desktops and servers. ? Install, maintain and troubleshoot VMware ESX and virtual machines. ? Responsible for troubleshooting Desktop user issues and other Network devices like Printers, Scanners, etc. ? Configuring Cisco IP phones and Cisco Call Manager. ? Maintaining Proxy Server for enhancing Web Security and performance. ? Tuning firewall to control web traffic for organizational compliance. ? Managing the support and provision of project tools and equipment along with data security, software and license control. Additional Information Technical Skills Summary ? Expertise in Design, Implementation and Administration in diversified industries. ? Solid knowledge of information security principles and practices. Cryptography, Forensics, PenetrationTesting, Data Loss Prevention, Vulnerability assessments, Business Continuity, Application Security, legal issues and IT auditing. ? Experience in handling, complete Threat and Vulnerability Life-Cycle ? Sound knowledge and experience in SIEM, host and network based intrusion detection for log analysis to determine the threat pattern, attacks and anomalies on the network. ? Installation, configuration, monitoring and response to security system incidents. ? Understanding of advanced security protocols and standards ? Experience with software and securityarchitectures ? Working knowledge of various forensics like Disk, Memory, Network, DNS, Mobile, Malware reverse-engineering, etc. ? Proactively assesses potential items of risk and opportunities of vulnerability in the network. ? Experience with securitypractices of Intranet and Extranet. ? Working knowledge on OWASP Top 10 Risks. ? Good knowledge on vulnerabilitymanagement tools ? Good exposure with compliances like PCI, HIPAA, SOX, FISMA and NIST. Technical Skills Category Skills/ Tools Networks Cisco, Juniper - Routing / Switching, Cisco, Checkpoint - VPN, Cisco, F5 - Load-balancers, Cisco, Silverpeak - Wan-Optimizers, Cisco, Juniper, PaloAlto - Firewalls Security Qradar, Splunk, Loglogic, Sophos, Proofpoint Email Security, Infoblox DNS, Symantec MSS, Dell Secureworks MSS, Symantec SIEM, Symantec DLP, Rapid7 Vulnerabity Scanner, Nessus, Metasploit, Altiris, CoreImpact, Symantec Data Center Security, Tanium endpoint security, User behavior analytics, Qualys Forensics / Malware SysInternal, Yara / OpenIOC, Encase Cyber, Resolution1 CIRT, Access data, REMnux, Volatility, Redline Others KALI Linux, Bash Script, Windows PowerShell, Python, Windows Active Directory, HTML, SQL Server, VMware, Virtualbox,

Name: Bruce Kim

Email: scott49@example.net

Phone: 001-408-261-6479x072