**Sharjeel Waheed** 

**Visa: Green Card**

[**Clark@softnice.com**](mailto:Clark@softnice.com) **|6103431448**

* bd10358_
* **PROFESSIONAL SUMMARY:**
* Extensive experience in Architecting and deploying various components within Splunk (indexer, forwarder, search head, deployment server) and security delivering innovative solutions to fix around and automation.
* Experience in **configuring, implementing, analyzing and supporting Splunk server infrastructure** across Windows, UNIX and Linux. Experience with a variety of **Operating Systems, Protocols and Tools** depending on the type of platform or application to be administered.
* **Upgrade and Optimize Splunk** setup with new discharges.
* Extensive experience in deploying, configuring and administering **Splunk clusters**.
* Expertise in **Actuate reporting, development**, deployment, management and performance tuning of Actuate reports
* Knowledge of Computer Networking Basics, **SOC Components, OSI model, TCP/IP protocols, Data Backup basics, Information Threats and Attacks.**
* Created **Splunk app** for **Enterprise Security** to identify and address emerging security threats through the use of continuous monitoring, alerting and analytics.
* Helping application teams in on-boarding Splunk and creating **dashboards, alerts, reports** etc.
* Experience working on Splunk 5.x,6.x, Splunk Enterprise Security 4.1, Splunk DBConnect1.x,2.x on distributed Splunk Environments and Clustered Splunk Environments on Linux and Windows operating systems.
* Worked in **SOC department** to analyse security incidents and log analysis
* Implementation of a GRC utility (from POC, through evaluation, selection, and implementation)
* Solid understanding and implementation of **Firepower and identity service** engine for big organizations
* Setup **Splunk Forwarders** for new application levels brought into environment.
* Develop custom app configurations (deployment-apps) within SPLUNK in order to parse, index multiple types of log format across all application environments.
* **System Administration** familiar with Windows Servers, Red Hat Linux Enterprise Servers.
* Good Understanding of configuration files, precedence and daily work exposure to **Props.conf, transforms.conf, inputs.conf, outputs.conf** and Setting up a forwarder information based on requirement.
* Build and configured a virtual data center in AWS cloud to support enterprise data warehouse hosting including VPC, public and private subnets, security groups, route tables
* Experience in Optimized search queries using **summary indexing.**
* Experience in Designing and implementing Trend Micro
* Analyzed AWS configuration logs, AWS Cloud watch flow logs.
* Enabling the Radius Authentication to administer the SSL VPN Box
* Well experienced in migrating data to AWS cloud.
* Excellent skills on troubleshooting and problem determination of **HTTP/System/ Network** related problems including monitoring, capacity planning and maintenance by providing 24X7 support on call for all mission critical applications. Strong background in a disciplined software development life cycle (SDLC).
* Excellent analytical and interpersonal skills and ability to learn new concepts and supported 24/7 on call in production and development environment.
* Understanding of Network Firewalls, Load-balancers, LDAP and complex network design.
* Experienced with security-related technologies including Active Directory, host-based firewalls, host-based intrusion detection systems, application white listing, server configuration controls, logging, SIEM, monitoring tools, and antivirus systems.
* Worked with members of the Security Operations Center to provide guidance and assist with remediation plans for incidents and discovered vulnerabilities.
* Have experience working in different environments and with the process flows in **AGILE** as well as Waterfall methodologies.
* Used Machine learning to solve major logs, events and metric issues in ITSI application in Splunk environment.
* Excellent Communication Skills and Presentation Skills, Comprehensive problem solving abilities.
* Interpreted and developed **SIEM products** to meet the internal and external and customer requirements. Experience in working on Enterprise Security log management and SIEM solutions.
* Created dynamic thresholds and where able to identify root cause of the issue using ITSI application.
* Worked on Security solutions SIEM that enable organizations to detect, respond and prevent these threats by providing valuable context and visual insights to help you make faster and smarter security decisions.
* Expertise with SIEM (security information and event management). Manage Splunk user accounts (create, delete, modify, etc.) Scripted SQL Queries in accordance with the Splunk.
* Maintain current functional and technical knowledge of the Splunk platform and future products.

**Skills**

|  |  |
| --- | --- |
| Log Analysis Tool | Splunk Enterprise Server 5.x/6.x/7.x, Splunk Universal Forwarder 5.x/6.x, Splunk DB Connect |
| Web/App Servers | Web Sphere Application Server 5.0/6.x/7.x/8.x, Web Sphere MQ Sever 6.x/7.x, WebSphere XD 6.0/6.1, IBM Http Server 6.x/7.x/8.x, Apache Web Server 2.x, Tomcat 5.5, IIS 6/7.x |
| Operating Systems | IBM AIX (5.1/6.1), RHL Linux, Windows Server 2003/2008 R2, VMWare |
| Programming | Java, J2EE, C++, C, SQL/PL SQL, HTML, DHTML, XML. |
| Scripting | JACL, Python, WSCP, WSADMIN, Korn Shell Script, Perl, JavaScript, CSS, Batch |
| Networking | TCP/IP Protocols, Socket Programming, DNS. |
| Frame work | MVC, J2EE Design Patterns, Struts. |
| IDE | Eclipse, RAD 7, Net Beans, Edit plus, TOAD |
| Others | Site Minder r6/r12/r12.5,Ping Federate 6.X,7.X |

**CERTIFICATION**

* **CompTIA Cyber Security Analyst (CYSA+)**
* **Cisco Certified Network Associate (CCNA)**
* **Cisco Routing and Switching**

**PROFESSIONAL EXPERIENCE:**

**ShopDafe, Oct 2018 - Present**

**San Francisco, CA**

**Sr. Cyber Security Analyst**

**Responsibilities:**

* Responsible for monitoring and, providing analysis in a 24x7x365 using various SIEM, IDS/IPS tools.
* Verify that the Windows Virus Definitions on the SEPM are within 24hours from those reported by Symantec cloud security.
* Experience on Network scanning and penetration testing (BurpSuite) using various web application security tools like Metasploit, OWASP ZAP Proxy, Nmap, Qualys and Rapid 7.
* Involved in setting up alerts for a different type of errors, Data Enrichment using the lookups and Data Interpretation using the Fields and Fields Extraction and performing the Data Normalization using the Tags.
* Good Understanding of configuration files, precedence and daily work exposure to Props.conf, transforms.conf, inputs.conf, outputs.conf and Setting up a forwarder information based on requirement.
* Maintained Splunk Environment with multiple indexers; managed and configured settings.
* Improved search performance by configuring to search heads for all Indexes in production.
* Analyzed security based events, risks and reporting instances. Developed Splunk queries and dashboards targeted at understanding application performance and capacity analysis.
* Expertise in development of Information Security Programs based on frameworks such as NIST 800-16, NIST 800-50, NIST 800 -53 , 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.
* Using proofpoint to analyze the alerts received in order to understand the header details received from phishing and take necessary actions to block the url or sender.
* Creating case for the suspicious issue and forwarding it to Onsite SOC team for further investigation.
* Worked as Incident Co-ordinator resource covering Event & Incident analysis, investigation and closure of events reported by Security Operational Centre (SOC)
* Worked for getting data in managing Splunk apps. Assisted internal users of Splunk in designing and maintaining production-quality dashboards.
* Splunk DB Connect 2.0 in search head cluster environments of Oracle. Installation and implementation of several kinds of visualizations to Splunk dashboards.
* Continuous monitored of the alerts received through emails to check if all the application servers and web servers are up.
* Worked with governance and risk compliance, identity and access management, host and network security team to analyze the root cause of an alert.
* Responsible for monitoring and, providing analysis in a 24x7x365 Security Operation Center (SOC) using Splunk SIEM, IDS/IPS tools.
* Knowledge on Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing.
* Ability to build custom applications and technical add-ons for efficiently on-barding data and meeting Splunk CIM compliance for Enterprise Security accelerated data models
* Conducted surveillance on various phishing emails and created alerts from future spam. Worked as part of Cyber Security Incident Response team to check on malware virus and threat emails.
* Developed Splunk Search Processing Language (SPL) queries, created Reports, Alerts and Dashboards and customized them.

**Environment**: Splunk.7.x, Splunk 6.x, Splunk DB Connect and other modules, Oracle WebLogic 9.x/10.x, Tomcat 5.x/6.x, Oracle 9i/10g, Solaris 10, LINUX, Sun ONE Directory Server 6, Sun One Web Server 6.0, Apache 2.x, Python

**Horizon BCBS Feb 2016 – Sep 2018**

**Jersey City, NJ**

**Cyber Security Specialist**

**Responsibilities:**

* Installation and configuration of Splunk product at different environments. Configured Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management.
* Monitoring or analyzing the real-time events for the security devices like Firewall, IDS, Anti-Virus etc., using SIEM tools.
* Proficient in designing and deploying large scale applications by using almost all of the AWS stack (Including EC2, Route53, S3, RDS, Dynamo DB, SNS, SQS, IAM) focusing on high availability, fault tolerance, and Auto Scaling in AWS Cloud Formation
* Upgraded Splunk Enterprise from v 6.2 to v 6.5.1 in clustered environments and non-clustered environments.
* Analyzed security based events, risks and reporting instances. Correlating events from a Network, OS, Anti-Virus, IDS/ IPS, Firewalls or Proxies and analyzing them for possible threats.
* Understand and interpret customer requirements for Splunk implementation for an enterprise solution.
* Assist with the development of process and procedures to improve incident response times, analysis of incidents, and overall SOC functions.
* Provided real time intrusion detection host-based monitoring services using McAfee EPO and Carbon Black.
* Worked on SOC department which runs 24\*7 days and able to analyse all security incidents
* Experience with creating Physical and logical data models
* Developed Splunk Infrastructure on Cloud (Amazon AWS) in coordination with infrastructure Support Teams.
* Worked on Splunk ITSI scales to collect and index terabytes of real-time and historical events and metrics, that are both human and machine- generated, across multi-datacenter and cloud-based infrastructures.
* Provide deployment strategies with the understanding of affordable risk based on customer acceptance.
* Experience in building / deploying complex infrastructure & proven hands-on cloud migration solution design / delivery experience, advised software development teams on architecting and designing web interfaces and infrastructures that safely and efficiently power the cloud environment
* Created and configured management reports and dashboards. Planned, implemented, and managed Splunk for log management and analytics
* Monitor security violations, flag potential violations and logging security incidents in Service Now.
* Validate the existing rules and provide recommendation on fine tuning the rules. Creating and sending Risk Advisories to our clients.
* Working as Analyst SOC Operations for monitoring, analyzing logs from various Security
* Research for various **PKI** related technologies
* Responsibility for the planning and controlled execution of releases into the managed environment
* Performed vulnerability scanning on web applications and databases to identify security threats and vulnerabilities.
* Conduct **FISMA complaint security control assessments** to ascertain the adequacy of management, operational, technical and privacy controls.
* Conducted system security assessments based on **FISMA, NIST and HIPPA/PCI DSS Compliance**.
* Suppress false positive alerts. Weekly/Monthly incident analysis report. Analyzing the events and providing solutions for the incidents.
* Involved in setting up alerts for a different type of errors, Data Enrichment using the lookups and Data Interpretation using the Fields and Fields Extraction and performing the Data Normalization using the Tags.
* Maintained Splunk Environment with multiple indexers; managed and configured settings.
* Improved search performance by configuring to search heads for all Indexes in production.
* Analyzed security based events, risks and reporting instances. Developed Splunk queries and dashboards targeted at understanding application performance and capacity analysis.
* Work with SIEM tool QRadar by tuning security events, creating building block, search for reports and search security events.
* Worked for getting data in managing Splunk apps. Assisted internal users of Splunk in designing and maintaining production-quality dashboards.
* Used Machine learning to solve major logs, events and metric issues in ITSI application in Splunk environment.
* Splunk DB Connect 2.0 in search head cluster environments of Oracle and support, configure, Installation and implementation of several kinds of visualizations to Splunk dashboards.
* Continuous monitored of the alerts received through emails to check if all the application servers and web servers are up.
* Worked in SIEM environment Implemented security systems to computer networks in compliance with company's security policies. Prepared documents to support customers and service engineers.
* Knowledge on Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing.
* Conducted surveillance on various phishing emails and created alerts from future spam. Worked as part of Cyber Security Incident Response team to check on malware virus and threat emails.
* Developed Splunk Search Processing Language (SPL) queries, created Reports, Alerts and Dashboards and customized them.
* Used Machine learning to solve major logs, events and metric issues in ITSI application in Splunk environment.

**Environment**: Splunk 6.x, Splunk DB Connect and other modules, Oracle WebLogic 9.x/10.x, Tomcat 5.x/6.x, Oracle 9i/10g, Solaris 10, LINUX, Sun ONE Directory Server 6, Sun One Web Server 6.0, Apache 2.x, Python

**SyncGrw InfoTech Mar 2014 - Nov 2015**

**Pakistan**

**Cyber Security Admin**

**Responsibilities:**

* Assessed and reviewed current technology infrastructure to identified **key risk areas** and ensured a level of control was in place to handle those risks.
* Deployed and configured McAfee products for client.
* Functioned as a SME for McAfee suite of products like McAfee ePO, McAfee Endpoint Encryption, McAfee DLP Endpoint
* Responsible for the research, design, engineering and implementation of Security Incident Response tools.
* Assisted design and implementation of network simulation environment (sandbox) using tools like NS-3, OPNET.
* Used IBM Rational Appscan, Acunetix, Qualys, w3af for reducing risk by testing web applications prior to deployment and for ongoing risk assessment in production environments
* Exhausting Symantec DLP to monitor the transmission of confidential data (PII) contained in corporate emails that were sent using Microsoft Exchange.
* Public and private cloud software defined networking – Amazon Direct Connect, AWS VPC, Azure ExpressRoute, VMware NSX, Palo Alto
* Configuring rules and maintaining Palo Alto Firewalls & Analysis of Firewall logs
* Delivering secure architecture designs in Public Cloud including AWS, Azure, and Google Cloud Platform
* Own all aspects of cloud security product definition including vendor integration, platform integration and monitoring for cloud platforms including but not limited to AWS and Azure Cloud
* Experience in installing, configuring, managing and troubleshooting SourceFire IPS appliances and ensuring security appliances are up to date with the latest OS, Patches, Symantec DLP, McAfee ePO, Cisco, Signature updates, and vulnerability database updates.
* Development and formulation of specifications for computer programmers to use in coding, testing, and debugging of computer programs and deploying on variety of operating systems (Windows, Linux or UNIX variants).
* Senior Security Incident Response Liaison to 52 acquired businesses. Provide consulting and incident response services to our partners and our core international companies and entities
* Conducted network and server vulnerability assessment scans plus track and report risk mitigation using **Nessus OpenVAS**, for systems monitoring and operations environment.
* Worked with Symantec DLP upgrades and patches
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP), forensics, sniffers and malware analysis tools.
* Implemented multiple tools including Symantec DLP, and QRadar SIEM
* Exhausting Symantec DLP to monitor the transmission of confidential data (PII) contained in corporate emails that were sent using Microsoft Exchange.
* Supported in the monitoring and setting policies in EPO server, maintain updates on HBSS server, domain servers, and domain workstations, push McAfee policies to required computers, and Symantec to servers
* Through teamwork, conducted security incident investigations; sniffing network traffic for unauthorized network services; reviewed and authorized request for network services such as. Modem lines, ISDN, remote access, **VPN, Internet access (ISS Web filtering), and Verisign PKI.**
* Maintained, monitored, and upgraded the **IDS system** and created custom daily reports to alert on anomalous traffic patterns and behaviors, which proved valuable in curtailing the spread of malware and mitigating Worm outbreaks using **BRO IDS, Suricata IDS**.
* Used Reverse engineering tools to such as **IDA Pro, OllyDbg,** and **Imagix**.
* Supported Cybersecurity Innovation Lab with the implementation of Tripwire Enterprise and IP 360
* Administered asset reconciliation with Tripwire
* Set-up Snort as preferred IDS/IPS to log inbound and outbound connections for traffic analysis and packet logging.
* Provide subject matter expertise with regard to applicable regulations such **as PCI DSS, NIST-SP800-53, and ISO Risk assessment** for best practice throughout all phases of corporate projects.
* Coordinating and supporting the implementation of the response strategies with other parts of the enterprise or constituency, including IT groups and specialists, physical security groups, information security officers (ISOs), business managers, executive managers, public relations, human resources, and legal counsel **using Log Analysis, Log Management.**
* Conducted risk assessment evaluating security of Web applications and related infrastructure, defining risk matrix, providing technical and executive reports with detailed findings, recommending mitigation strategies and performing cost-benefit analysis
* Conducted Web security related incident responses while supporting investigations of security violations
* Experience with Google Suit / Drive, Microsoft office programs including Word, Excel, Outlook, Project, Visio, and PowerPoint and with other industry standard computer program