**CHETAN TRIVEDI**

(414)-522-7414 • 5250 Town and country Blvd, Frisco, TX  75034 • rockytrived@yahoo.com



**SUMMARY**

* Computer Science Engineer with previous professional experience. Detail-oriented individual with patience and flexibility that thrives in a position that requires quick learning and great accuracy. Proficient Splunk Engineer with 4 year of IT experience in client/server applications.

**EDUCATION**

Master of Science in Computer Science (MSCS), Northwestern Polytechnic University May 2015

Specialization - Cyber security, Advance Unix programming.

Bachelor of Technology (B. Tech), Jawaharlal Nehru Technological University May 2011

Specialization – C, C++, Java, Unix.

**Certification and Training:**

Splunk Certified Power User.

CompTIA Security+ Certification.

**Awards:**

Dell Excellence Award.

**Tools:**

|  |  |  |
| --- | --- | --- |
| Splunk 6.5/6.6,ITSI, Nagios, App dynamics, Wireshark, FireEye, McAfee ePO, ELK. | Windows Server 2012/2008/2003R2, Linux Redhat and Unix Servers, ServiceNow, F5 data ASM, TCP/IP,Share point, cisco routers, MS Office. | HTML, XML, CSS, JavaScript, JAVA, JQuery, Angularjs, Linux, shell, bash scripting. |

**Professional Experience:**

**Dell Services, Plano, TX Sep2016 to till date**

**Network Security Sr. Splunk Admin**

* Provide regular guidance to Splunk project teams on complex solution and issue resolution.
* Created Dashboard, report, scheduled searches and alerts.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across Unix and Windows platforms.
* Maintain, grow and improve the TVX Splunk environment.
* Integrated Service Now with Splunk to generate the Incident from Splunk.
* Worked on DB Connect configuration for Oracle, MySQL and MSSQL.
* Deploy, configure and maintain Splunk forwarder in different platforms.
* Creating Reports, Pivots, alerts, advance Splunk search and Visualization in Splunk enterprise.
* Manage Splunk configuration files like input, props, transforms etc.
* Upgrading the Splunk Enterprise and security patching.
* Worked on splunk CIM implemented add on that contains collection of data models. Normalizing data with CIM( common information model), developed reports, correlation searches and dashboards to present a unified view of a data domain.
* Working on Shift basis in SOC, giving client 24/7 service, monitoring.
* Loaded skills like understanding security policies, Change Management Process, Domain Name Service (DNS), Data & traffic analysis, identifying security events, incident response, IP addressing.
* Also in incident response team responsible for handling security that occur within organization and correcting and documenting the security issue in a timely manner.
* Ingesting and working with various data types like CSV, JSON, XML, Raw Logs, syslogs and parsing them with custom source types.
* Working knowledge on security technologies like Encryption, Data Loss Prevention (DLP), IPS/IDS etc.
* Actively protects the availability, confidentiality, and integrity of customer, employee, and business identity.
* Contribute to the Risk Assessment Program including identifying and scoring risk.
* Collaborate with the team and architecture on new platforms, IAM roadmap, assess security risks, and identity long-term strategy recommendations.
* Position requires mentoring and training of SOC Technicians and SOC employees.
* Monitored and correlated events with thorough knowledge of principles, methods, and techniques of network and data security.
* Experience working on Cisco Firewalls, Palo Alto Networks Firewall.
* Provide scalable, supportable military grade TCP/IP security solutions along with expert TCP/IP network designs that enable business functionality.

**Environment**:  Windows Server 2012/2008/2003R2, Linux and Unix Servers, SPLUNK 6.4/6.5, ServiceNow, F5 data ASM, TCP/IP, Cisco Firewalls (ASA 5505, 5506-X, 5585), Palo Alto Networks Firewall models (PA-2k, PA-3kand PA-5 k).

**Synchrony Financial, Chicago, IL March2016 to Sep 2016**

**Splunk Admin**

* Design, support and maintain the Splunk infrastructure on Windows, Linux and UNIX environments.
* Installation of Splunk Enterprise, Splunk forwarder, Splunk Indexer, Apps in multiple servers (Windows and Linux) with automation.
* Splunk Heavy Forwarder Configuration. Install and maintain the Splunk add-on including the DB Connect, CIM, Active Directory, LDAP for work with directory.
* Foundation skills like, Device config, traffic capture, performance monitoring, device monitoring.
* Monitor systems and report the status to client staff.
* Splunk server configurations (web, indexing retention, authentication, etc.), data onboarding operations, data parsing operations.
* Worked on ITSI service analyzer KPI’s.
* Upgrading threshold templates in ITSI, health check inquires. Creating multi kpi alert to configure email alert in ITSI.
* Creates correlation search rule for the admin activity, indexes for field extractions.
* Manage Splunk configuration files like input, props, transforms etc.
* Upgrading the Splunk Enterprise and security patching.
* Well versed in both remote and on-site user Splunk Support.
* On boarded multiple data sources within Splunk, creating custom TAs for data parsing.
* Advised clients on the best practices for a Splunk deployment.
* Developed detailed documentation for the installation and configuration of Splunk and Splunk Apps.

**Environment:**  Windows Server 2012/2008/2003R2, Linux RedHat, Linux and Unix Servers, SPLUNK 6.5, Splunk CIM, ServiceNow, F5 data ASM, wireshark, Jira, TCP/IP, CompTIA Security+.

**Northwestern Mutual Insurance (Milwaukee, WI) May2015 to March2016**

**Splunk Admin**

* Monitor systems and report the status to client staff.
* Good working knowledge on AWS Environment, Cloudtrail, Cloudwatch, Vpc flow logs, EC2 instance, configuring AWS.
* Splunk server configurations (web, indexing retention, authentication, etc.).
* Splunk data onboarding operations (inputs, SQL, index-time configurations).
* Splunk data parsing operations (search-time field extractions, event types, tags).
* Manage existing application and create new applications (visual and non-visual).
* Worked on AWS cloudtrails and F5 data.
* Deploy, configure and maintain Splunk forwarder in different platforms.
* Creating Reports, Pivots, alerts, advance Splunk search and Visualization in Splunk enterprise.
* Provide power, admin access for the users and restrict their permission on files.
* Installed and upgraded Splunk software in distributed and clustered.

**Environment**:  Windows Server 2012/2008/2003R2, Linux and Unix Servers, SPLUNK 6.5, ServiceNow, F5 data ASM, wireshark, AWS cloudtrail, cloudwatch, Jira, TCP/IP, CompTIA Security+.

**Multitude 9fx, Hyderabad, India. March 2012 – May 2013**

**Network Security Analyst.**

**Responsibilities:**

* Analyze security and Firewall logs for compromised/infected host on the network.
* Responsible for Disaster Recovery Site Management.
* Design and develop the Security Zone diagram for the Security Monitoring Team.
* Member of the Security Operations Center (SOC) that provides 24/7 monitoring, analysis and remediation of security events.
* In charge of Cyber Attack Response Team including data recovery.Analyze security incidents and escalate as necessary.
* Create daily, monthly and adhoc reports for various devices.
* Extensive understanding of networking concepts, (IE. Configuration of networks, router configuration and wireless security, TCP/IP, VPN, Content Filtering, VLANs, and routing in LAN/WAN, Ethernet Port, Patch Panel and wireless networks.)
* Identify, monitor and prepare daily reports of Network threats and Vulnerabilities.
* Familiar with ISO, PCI other security frameworks. Familiarity with security analysis techniques.
* Prepare reports using the Nagios server monitoring tool.
* Create new process document to help the Analysts in analysing events.
* Responsible for vulnerability reporting and vulnerability scan scheduling.
* Manage and configure security applications, firewalls, anti-virus software.
* Follow up with asset owners for remediation of vulnerabilities either at OS or application level.Maintain Spam Filter and Web Filter.
* Work with vendors to support system maintenance, Keep servers updated with latest security updates, Create and migrate virtual servers.