Splunk Engineer Splunk Engineer Splunk Engineer - ConocoPhillips Bartlesville, OK Professional with around 8+years of experience in IT industry comprising of Splunk Installation, Splunk architecture and components including search heads, indexers and forwarders. Worked on multiple security tools such as Phish Me, Cisco ISE, CarbonBlack Protect and Defense. Experience in implementation of other Splunk premium applications - ITSI, UBA, ES, Hunk. Expertise in customizing Splunk for Monitoring, Application Management, and Security as per customer requirements and industry best practice. Experienced in the implantation of Key ITSI features like Service Analyzer, Glass tables, Deep dives, Multi-KPI alerts, Episode Review and other ITSI modules. Hands-on experience with Splunk Core infrastructure (Forwarders, Indexers, Search Head Cluster Environment) Written customized Python scripts for specific conditions to trigger the alerts. Good Knowledge on Splunk User Behavior Analytics (UBA). Achieved hands-on knowledge of Splunk Searching and Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management. Good knowledge on Splunk ITSI Good understanding of networking concepts. Sharpened in field Extraction, using IFX, Rex Command, and Regex in configuration files. Supervised Splunk administering in environments like Window Servers, Red Hat Linux Enterprise Servers. Implemented the log correlation searches based on end client requirements. Worked on multiple security tools such as Phish Me, Cisco ISE, CarbonBlack Protect and Defense. Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls. Implemented the indexer clustering and search head clustering in a production environment. Implemented workflow actions to drive troubleshooting across multiple event types in Splunk. Create Splunk Search Processing Language (SPL) queries, Reports, Alerts, and Dashboards. Analyze computer systems and mobile devices to identify malicious binaries and to discover evidence of any suspicious activities related to malware. Expertise in customizing Splunk for Monitoring, Application Management, and Security as per customer requirements and industry best practice. Provided in-depth behavioral and dynamic malware analysis to identify current infection trends. Monitoring network traffic for security events and perform triage analysis to identify security incidents. Focusing on learning DevOps

technologies in order to contribute more towards software development. Authorized to work in the US for any employer Work Experience Splunk Engineer ConocoPhillips - Bartlesville, OK April 2018 to Present Responsibilities: Improving diagnosing risk, security and compliance incidents with issues involving extensive analysis Assist to recommending security resolutions to management for better malware detection and endpoint security Introduced Search Head Clustering instead of pooling. Conduct Splunk Manual Health Check and identified the license violations. Review overall system configurations of all Splunk servers and services. Identify errors and misconfigurations, potential upgrades, changes to increase performance, changes in ingestion rates and retention times to improve indexing, and log filtering to maximize Splunk Licensing. Create new reports, metrics and dashboards. Onboard new data from various sources and Designing and building new log & data mining services including Planning, supporting of execution of assembling and Perform data mining and analysis, utilizing various queries and reporting methods. Requirement gathering and analysis. Interacted with team members and users during the design and development of the applications and Splunk Objects. Creating, maintain, support, repair, customizing System & Splunk applications, search queries and dashboards. Building Splunk queries by Splunk Search Processing Language (SPL) and Regular expressions. Data collection from various systems/servers, Forwarder Management, creating and managing Splunk apps. Good experience in working with SNMP traps and Syslog NG in onboarding the security devices on Splunk. Installed Splunk Common Information Model add-on is packaged with Splunk Enterprise Security, Splunk IT Service Intelligence, and the Splunk App for PCI Compliance. Install, configure, and troubleshoot Splunk. Experience with regular expressions and using regular expressions for data retrieval. Work with application owners to create or update monitoring for applications. Good experience in building Splunk Security Analytics. Lead logging enrollments from multi-tier applications into the enterprise logging platforms. Assist internal users of Splunk in designing and maintaining production-quality dashboards Ownership of the log & data mining service based on the Splunk product including This individual will also be expected to work with other departments, representing the team on all technical matters related to log monitoring and

analysis The Splunk engineer should be familiar with a Linux environment, editing and maintaining Splunk configuration files and apps. Configurations with deployment server, indexers, search heads, serverclass.conf, server.conf, apps.conf, props.conf, transform.conf, forwarder management configurations. Good experience in clustering, deploying apps through Splunk deployment server, deployer, Splunk version upgradation, creating roles and authentication. Created Summary searches and reports; In depth knowledge of Splunk license usage abd safeguarding from violation. APM-Splunk Developer Catholic Health Initiatives- CHI - Jacksonville, FL February 2016 to March 2018 Responsibilities: Designed Splunk Enterprise 6.5 infrastructure to provide high availability by configuring clusters across two different data centers. Installed, Configured, Maintained, Tuned and Supported Splunk Enterprise server 6.x/5.x. Architect and Implement Splunk arrangements in exceptionally accessible, repetitive, conveyed figuring situations. Performed Field Extractions and Transformations using the RegEx in Splunk. Responsible for Installing, configured and administered Splunk Enterprise on Linux and Windows servers. Supported the upgradation of Splunk Enterprise server and Splunk Universal Forwarder from 6.5 to 6.6. Installation and implementation of the Splunk App for Enterprise Security and documented best practices for the installation and performed knowledge transfer on the process. Worked on installing Universal Forwarders and Heavy Forwarders to bring any kind of data fields into Splunk. Writing Splunk Queries, Expertise in searching, monitoring, analyzing and visualizing Splunk logs. Experience in alert handling, standard availability and performance report generation. Experience in root cause analysis of post-production performance related issues through Splunk tool. Designing, optimizing and executing Splunk-based enterprise solutions. Installed and configured Splunk Universal Forwarders on both UNIX (Linux, Solaris, and AIX) and Windows Servers. Hands on experience in customizing Splunk dashboards, visualizations, configurations using customized Splunk queries. Monitored the Splunk infrastructure for capacity planning, scalability, and optimization. Experienced in using Splunk- DB connect for real-time data integration between Splunk Enterprise and rest all other databases. Expertise in Actuate Reporting, development, deployment, management and performance tuning of Actuate reports. Responsible with Splunk Searching and

Reporting modules, Knowledge Objects, Administration, Add-On's, Dashboards, Clustering and Forwarder Management. Monitored license usage, indexing metrics, Index Performance, Forwarder performance, death testing. Splunk Architecture/Engineering and Administration for SOX monitoring and control compliance. Design and implement Splunk Architecture (Indexer, Deployment server, Search heads, and Forwarder management), create/migrate existing Dashboards, Reports, Alerts, on daily/weekly schedule to provide the best productivity and service to the business units and other stakeholders. Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms. Configured Syslog server for the forwarding the logs to Splunk server via network protocols like TCP and UDP. Subject matter expert in best practices, security protocols, PKI, and other security-related issues. Monitored the database (data tables and error tables), WebLogic error log files and application error log files to track and fix bugs. Responsible for troubleshooting various indexing issues by analyzing Splunk logs such as splunkd.log, metrics.log ingested as internal index. Support and execute arrangements considering a full information lifecycle (Search & Investigate, Add Knowledge, Monitor & Alert, Report & Analyze). Followed agile and scrum process for the whole implementation process. Developed KPI's associated with a service and built glass tables, Deep Dives, Notable events. Configured services, Entities, Correlations searches with corresponding KPI metrics in splunk ITSI Application. Configured splunk for dynamic analytics and machine data indexing. Splunk DB Connect 2.0 in search head cluster environments by importing and exporting log data from databases like Oracle, MySql. Splunk Enterprise Deployments and enabled continuous integration on as part of configuration management. Configured and developed complex dashboards and reports on Splunk. Involved in Installation, Administration and Configuration of Splunk Enterprise and integration with local legacy systems. Expertise in creating and customizing Splunk applications, searches and dashboards as desired by IT teams and business. Drive complex deployments of Splunk dashboards and reports while working side by side with technical teams to solve their integration issues. Performed troubleshooting and/or configuration changes to resolve Splunk integration issues. Hands on development experience in

customizing Splunk dashboards, visualizations, configurations, reports and search capabilities using customized Splunk queries. Knowledge about Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License model. Responsible for documenting the current architectural configurations and detailed data flow and Troubleshooting Guides for application support. Managing indexes and cluster indexes, Splunk web framework, data model and pivot tables. Good experience in Splunk, WLST, Shell scripting to automate and monitor the environment routine tasks. Environment: Splunk 6.4.1, Splunk 7.1, AWS, AppDynamics, PACMAN, Jenkins, BitBucket, REST API's, CCP, PCF, Marathon, Python, Rally. Splunk Admin,Developer PricewaterhouseCoopers -PWC - Jacksonville, FL March 2014 to January 2016 Responsibilities: Daily Splunk administration maintenance. Established On-boarding of Web and database server logs into Splunk by DB Connect Application. Achieved hands-on experience in clustering, deploying apps through Splunk deployment server, Splunk version upgradation, creating roles and authentication. Utilized the Splunk Machine Learning concepts, algorithms to write complex queries using SPL and visualize data into dashboards and reports. Hands-On experience on multiple configuration file (.conf) settings. Configured the heavy forwarder to send the logs from QRadar server to Splunk indexers and customized the reports and dashboards. Involved in ingesting the data from multiple appliances into the cluster and analyze data with SPL queries. Splunk Administration and analytics development on Information Security, Infrastructure, and Network, data security, Splunk Enterprise Security app, Triage events, Incident Analysis. Developed specific content necessary to implement Security Use Cases and transform into correlation queries, templates, reports, rules, alerts, dashboards, and workflow Deployed Splunk enterprise package and forwarder package in multiple instances. Involved in standardizing Splunk forwarder deployment, configuration, and maintenance on all Windows and Linux platforms. Real-time monitoring of enterprise endpoints for signs of malicious activity by Carbon Black (CB). Analysed threat patterns by Carbon Black (CB) and investigate SIEM alerts with endpoint context and take actions if necessary. Participated in client requirements meetings and presented the visual presentations of possible outcomes. Developed

the use cases for different business requirements. Executed daily vulnerability assessments, threat assessment, and mitigation and reporting activities in order to safeguard information assets and ensure protection has been put in place on the systems. Designed the Correlation searches for multiple end client requirements. Extensive knowledge in creating accurate reports using XML, Dashboards, visualization, reports, alerts and pivot tables for the business users. Hands-on experience with Citrix NetScaler load balancer Hands-on experience with indexer clustering and search head clustering in both test and production environment Assisted the privileged user access management team to solve the daily encountered problems. Customization of Dashboards and reports and scheduled searches. Experience with working on Service now ticketing tool. Worked on User access roles and capabilities. Environment: Splunk 6.5.3, Linux, Windows 2008,2012, IBM AIX, Oracle11g, MS SQL Server 2012, SQL, Symantec Endpoint (SEP), Tripwire IP-360, Service Now (ITAM), Carbon Black(CB). Splunk , Security Analyst Health First - Birmingham, AL October 2012 to February 2014 Responsibilities: Experience in creating Splunk apps, searches, Data models, dashboards, and Reports using the Splunk query language. Splunk DB Connect 2.0 in search head cluster environments of Oracle, MySQL. Setup and configuration of search head cluster with three search head nodes and managing the search head cluster with deployer. Performed data onboarding from API's, HTTP Event collectors, Heavy Forwarders, Universal Forwarders, TCP and UDP ports etc. Experienced with logging of security-related technologies including Active Directory, host-based firewalls, host-based intrusion detection systems, application white listing, server configuration controls, SIEM, monitoring tools, and antivirus systems. Experience in using scripting languages. Created Dashboards, report, scheduled searches and alerts. Collecting data on attacks to help SOC engineers create reports for auditing purposes. Building the use cases and perform the tuning of rules and build the logic to mitigate the risks. Analyzed security-based events, risks and reporting instances. Onboard new log sources with log analysis and parsing to enable SIEM correlation. Creating and managing app, create a user, role, permissions to knowledge objects. Creating Vulnerability Assessment dashboard and that aggregates data across multiple services to identify critical threats and proactively mitigate

risks. Parsing, Indexing, searching concepts, Hot, Warm, Cold, Frozen bucketing and Splunk clustering. Worked on setting up Splunk to capture and analyze data from various layers Load Balancers, Web servers, and application servers. Scripted SQL Queries in accordance with the Splunk. Created many of the proof-of-concept dashboards for IT operations, and service owners which are used to monitor application and server health. Environnent: Splunk, WebLogic server 8.x/9.x/10.x/11g, Tomcat 6.0, IBM HTTP Server, Microsoft IIS 7.0, Windows 2008, web services, LDAP, web services, JDK 1.7, HTML, and XML. Splunk , IT Security Engineer Cyber Chasse - Dallas, TX July 2010 to September 2012 Responsibilities: Requirement gathering and analysis. Interacted with team members and users during the design and development of the applications and Splunk Objects. Creating, maintain, support, repair, customizing System & Splunk applications, search queries and dashboards. Building Splunk queries by Splunk Search Processing Language (SPL) and Regular expressions. Data collection from various systems/servers, Forwarder Management, creating and managing Splunk apps. Good experience in working with SNMP traps and Syslog NG in onboarding the security devices on Splunk. Installed Splunk Common Information Model add-on is packaged with Splunk Enterprise Security, Splunk IT Service Intelligence, and the Splunk App for PCI Compliance. Install, configure, and troubleshoot Splunk. Experience with regular expressions and using regular expressions for data retrieval. Work with application owners to create or update monitoring for applications. Good experience in building Splunk Security Analytics. Lead logging enrollments from multi-tier applications into the enterprise logging platforms. Developed specific content necessary to implement Security Use Cases and transform into correlation queries, templates, reports, rules, alerts, dashboards, and workflow. Splunk Administration and analytics development on Information Security, Infrastructure and network, data security, Splunk Enterprise Security app, Triage events, Incident Analysis. Developed Splunk Objects and reports on Security baseline violations, Non-authenticated connections, Brute force attack's and many usecases. Receiving promptly, handling, gathering requirements through remedy tickets and resolving at on time. Experience creating and maintaining Splunk reports, dashboards, forms, visualizations, alerts. Splunk SPL (Search

Processing Language) and Dashboarding/Visualization. Setup dashboards for network device logs. Configurations with deployment server, indexers, search heads, serverclass.conf, server.conf, apps.conf, props.conf, transform.conf, forwarder management configurations. Good experience in clustering, deploying apps through Splunk deployment server, deployer, Splunk version upgradation, creating roles and authentication. Created Summary searches and reports; In depth knowledge of Splunk license usage abd safeguarding from violation. Environment: Splunk, Deployment server, Integration, Splunk 6.x Dashboard Examples, Server management, Dashboards, Search processing language (SPL), Field extraction, Regex, Rex, LINIX, XML. Education Bachelor's ..... Skills Db2, Machine learning, Splunk, Css, Tomcat Certifications/Licenses Driver's License

Name: Thomas Kent

Email: alvarezcharles@example.com

Phone: 229-930-7177x091