Sr. Technical Analyst -Arcsight Sr. Technical Analyst -Arcsight Sr. Technical Analyst -Arcsight Mountain View, CA Work Experience Sr. Technical Analyst -Arcsight Mischel Kwon & Associates, LLC September 2018 to November 2018 Develops/maintains use cases and SIEM content ? Deploys/maintains security sensors and tools ? Monitors security sensors and reviews logs to identify intrusions ? Reviews vulnerabilities and tracks resolutions ? Reviews and processes intelligence reports ? Assists with incident response ? Creates and delivers customer reports ? Participates in security/engineering issue resolution ? Assists with security assessment reports ? Assists with table top exercises Sr. Technical Analyst, Splunk Mischel Kwon & Associates, LLC February 2018 to September 2018 Expansion of Splunk architecture with more than 1000+ forwarders with two Deployment server ? Created a holistic architecture with more than 2000+ forwarders and 4 indexers in a single site cluster with 2 individual Search heads. ? Knowledge in designing Index Replication factor and Search factor ? Experienced in calculating storage space and predict the Indexer Hardware requirements ? Experienced in calculating the bucket based parameters for index ? Knowledge in maintaining Indexer Cluster with maintenance mode and offline modes ? Managed Splunk Indexer Cluster components ? Configured Splunk throughput rate, web enabling parameters ? Installed and configured syslog-ng for forwarding logs to Splunk indexer. ? Designed Splunk Heavy Forwarder to parse and filter the data. ? Implemented Splunk configurations in HF to mask the customer sensitive information ? Designed configurations to remove garbage data before processed into index queue ? Designed configurations to override the default metadata information at HF level ? Deployed basic queries using generating search commands like stats, chart, time chart, tables etc. ? Expertise in creating and managing Splunk based weekly and monthly reports with email outs ? Expertise in creating Splunk based Scheduled Alerts to trigger email notificiation in case of abnormalities ? Created Splunk Alerts to identify malicious intrusions in Application environment ? Knowledge in deletion of index using delete and clean data options Environment: Splunk Enterprise Server 5.x.x/6.x.x, Universal Splunk Forwarder 5.x.x/6.x.x, RedHat Linux, XML Senior Security Administrator - Arcsight International Monetary Fund (IMF) - Washington, DC December 2017 to January 2018 Administration of Arcsight Appliances ?

Upgrade Collector appliances and console ? Certificate Management Senior Security Architect- QRadar, PaSeries, Bit9, QualysGuard IBM Consulting May 2015 to September 2017 Designed, Developed, Provisioned and Managed several Log Sources - traditional and custom through uDSM/LSX ? Correlation rules to capture security offenses, and developed customized security offense monitoring reports ? Manage diverse QRadar appliances and Administration ? SIEM EPS tuning of the distributed deployment architectures ? Responsible for managing Vulnerability reports from multiple sourcesEnhanced the design of Flow sources on edge and internal and completed deployment ? Implemented Organizational SIEM policy - Enforced and implemented collection of event logs for Windows infrastructure to report through Wincollect ? Integrated Threat Advisories (X-Force and other advisories) and designed controls to proactively monitor for attacks ? Maintain the most recent QRadarUpgrade/Patches and apps for threat monitoring (most recent WannaCry, Petya, malware dectedtion and alert) Senior Security Architect- QRadar, Tipping Point IPS, Bit9, QualysGuard, TrendMicro OfficeScan STATE FARM MUTUAL INSURANCE - Bloomington, IL August 2014 to May 2015 BLOOMINGTON, IL 08/14 - 5/15 Senior Security Architect- QRadar, Tipping Point IPS, Bit9, QualysGuard, TrendMicro OfficeScan ? QRadar SIEM v7.2 Administration with SIEM EPS tuning, distributed deployment architectures ? Part of deployment team where parsing several Log sources are integrated into QRadar through mid-layer such as F5 for PCI and Syslog services. ? QRadar Vulnerability manager and Threat Manager (QVM and QTM) ? Added few Custom Log Sources via Universal DSM/LSX - QID adding/mapping and creating building blocks/rules. ? Created custom searches, custom reports, rules, reference sets and reference maps. Senior Security Architect- QRadar, Tipping Point IPS, Bit9, QualysGuard, TrendMicro OfficeScan SEARS HOLDING CORPORATION - Hoffman Estates, IL March 2013 to July 2014 HOFFMAN ESTATES, IL 03/13 - 7/31/14 Senior Security Architect- QRadar, Tipping Point IPS, Bit9, QualysGuard, TrendMicro OfficeScan ? QRadar Administration - Fine tune log sources sending events to Event processors, optimize asset DB, create custom event properties, optimize rules, reports, setup retention policies, tweak poorly written rules and document the periodic tweaks that needs to happen for a healthy performance * Using Security logs from different sources, investigate

security related incidents. These incidents ranged from recon, intrusions, malware, APT, DDoS, unauthorized access, and insider attacks that required an in-depth investigations * Building uDSM's for unsupported log types * Experience with QID adding/mapping and creating building blocks/rules. * Responsible for any critical updates patching, DSM updates and submit PMRs for any QRadar bugs * Creation of several Use Cases monitored by SOC and worked with Security operation center to investigate incidents while monitoring attacks on network - * few ex., heartbeat response, Citadel, ZAT, RAT, etc. * Created several reports for management, reports to monitor critical servers required for PCI/SOX * Creation of several custom fields that extracts key fields from log sources such as IDS/IPS (sensor location, Action taken for attacks), AV Trend Micro (Files affected, action taken), etc. ? Bit9 * Created policies for blocking, banning and white listing software * Created rules to take action based on rating and reputation ? QualysGuard * Vulnerability management and patching - feeds into QRadar Asset DB Consulting IT Security Expert Protecture Corporation - San Jose, CA August 2008 to May 2011 360 degrees, Seattle - SIEM & DLP consultant - Symantec DLP implementation, Arcsight SIEM ? DLP ? Assess DLP needs and recommend next steps ? DLP implementation design and deployment including data classification, data identification, reviewing network segments for protection, scope network gears and list high level ecosystem changes ? Initialize DLP implementation to align with management objectives and incident response process ? Policy creation and testing, Policy communication, Policy enforcement & Hand-off ? SIEM - Arcsight: ? Developed Arcsight rules, channels, and analysis methodology ? Wrote Use Cases to identify security events such as traffic from bad actors, AV failed recovery, malware attack, etc. ? Coordinated and conducted event collection, event management, compliance automation and identified monitoring activities through Arcsight ESM LondonFog (now Macys'), Seattle - DLP consultant - Websense DLP, Arcsight SIEM ? Performed risk assessment and data classification - customized existing DLP policies to re-align with data classifications and potential data leaks ? SIEM - Arcsight: Wrote Incident management playbook with ESM as the core tool ? Responded to day-to-day requests relating to Arcsight reports ? Tuned Arcsight ESM data quality to improve ISMS process efficiency ? Assisted other analysts using Arcsight and other tools to detect and respond to

IT security incidents. ? Wrote Use Cases to identify attacks such as Zero Access Trojan, Dictionary attack, etc. and worked with SOC to remediate in a timely manner ? Manage ISO-27001 program ? Manage Vendor security program EBAY - Consulting Vendor Risk Manager, Archer ? Responsible for Vendor Security Program - designed the vendor security policy based on the data classification of eBay. Designed semi-automated process to examine and categorize each vendor based on risk - designed vendor questionnaire based on SIG standards, designed the automated risk based vendor rating ? Using Archer, designed actionable triggers based on vendor supplied information to categorize risk-ranking of vendor management - Triggers included ordering the internal/external VA scans using QualysGuard ? Developed and Implemented vendor automation work flow (with Archer tools suite) ? Review QualysGuard reports to validate that the automated system categorization of vendor is appropriate and oversee the vulnerability remediation process SME, Security Incident Management Consultant FRANKLIN TEMPLETON, SAN MATEO May 2007 to June 2008 Review Information security incident reports and provide periodic management recommendations - Arcsight, Antivirus, IDS/IPS ? Perform threat based risk assessment IT Security Program Manager - Security Symantec Corporation - Cupertino, CA September 2006 to May 2007 2.0 Program * Responsible for Incident investigation and reporting - Manage escalations, review log data & Forensic reports * Managed the development and deployment of the most anticipated enterprise security project 'Threatcon XM' that takes the existing Threatcon to the next level. Threatcon XM is an enterprise service that delivers global security threats in real-time * Security Metrics development and reporting Senior Security Consulting Manager Protecture Corporation - San Jose, CA August 2002 to August 2006 My overall responsibilities included managing a team of IT Security consultants, deliver customer satisfaction & participate in pre-sales and post-sales customer meetings and advise customers of the IT Security Products IT Security Program Manager - Franklin Templeton * Led a team of Security Engineers to execute Security Incident investigation and Incident responses * Handled escalation, facilitated emergency meetings after reviewing and analyzing log data * Performed Forensic data capture for legal investigations * Developed ISO 17999 and ISO 27001 based Program to assess clients security posture and manage security projects * Analyze security

gaps to comply with SOX 404, SAS 70 and PCI regulations. * Led team to execute security audits - sample engagements below. Audit engagements Network and financial infrastructure Security Audit - Greater Bay Bancorp - Public company (NASDAQ - GBBK) * Hands-on auditing of clients network infrastructure - Firewall, Cisco Routers, IDS sensors, Web security, Active directory, TACACS, RADIUS, VPN, etc. * Hands-on auditing of financial platforms - Mainframe (AS400), Windows with Active directory. * Penetration tools: NetIQ security Analyzer, QualysGuard, Dumpsec, Velosecure. Compliance Engagements - Accomplishments for SOX, SAS70 and PCI/DSS clients: * Perform General Computer Controls (GCC) and Application Control review for Sarbanes-Oxley, Section 404 requirements * Auditing of SAP FI including User Master Record, negative postings, Profiles, authorization Objects, Program Access, Fields, Authorizations, Restricting access, services, work processes, system and custom transactions, ABAP programs, ABAP/4 Data dictionary, SAP user ids at operating system level, Change control directories, trace and log files and SAP customizing access * Performed security review of platforms including Windows/Unix, AS400, UNIX, PBX, Voice Response Unit, Cisco PIX firewall, Checkpoint Firewall Risk Management & Disaster Recovery engagements * Designed a comprehensive risk matrix for an Investment management company to address combination of technical, operational and procedural safeguards. Challenges included identifying and understanding networks, infrastructure, development and application level practices, global dissimilar practices and merger cultures for security, compliance and governance. Developed and implemented standard operating procedures for managers and senior managers for Windows, UNIX and network groups. Education Bachelor of Engineering in Engineering, EE BMS College of Engineering - Bengaluru, Karnataka 1990 Skills Splunk Certifications/Licenses CISSP, CISM

Name: Gerald Green

Email: mbaker@example.net

Phone: 001-263-527-9153x1735