Security and Risk Analyst lll Security and Risk Analyst lll Security and Risk Analyst lll - Gilead Sciences San Francisco, CA Around 7+ years of experience in Security information and Event management (SIEM) tools like Arc Sight, Splunk and Qradar. Around 2+ yrs. of experience with Vulnerability Management. Extensively worked on development and configuration of SIEM connectors for unsupported devices by HP ArcSight, RSA Security Analytics and Splunk to support controls monitoring and reporting. Installation of Connectors and Integration and testing of multi-platform devices with ArcSight ESM, Develop and test Flex Connectors for unsupported devices and Business applications. Having good knowledge of MS Active Directory. Hands-on with Nexpose Rapid7 and Symantec CCS. Experience on working with phishing emails Barracuda Spam filter. Monitoring web traffic using Cisco umbrella and Barracuda Web filter. Creating new policies to block suspicious domains in our environment. Worked with the UNIX/LINUX OS. Understanding of Python. Have experience on working with MS word, Excel, PowerPoint. Preparing for CEH certification. Performed proof of concept with ArcSight, Nexpose and RSA envision tools. Work Experience Security and Risk Analyst lll Gilead Sciences - Foster City, CA November 2017 to Present Responsibilities: Perform scans on assets in the environment and generate the vulnerability reports providing them to System Managers using Nexpose Rapid7. Aiding the team in designing and implementing an end to end vulnerability management process. Helping the users in remediating the vulnerabilities. Prepare adhoc reports to support system managers and Laboratory technology Operations Management to provide visibility. Applying exceptions/exemptions on vulnerabilities in Nexpose. Keep the patch management visibility dashboard updated. Preparing the Metrics report on vulnerabilities for the higher management. Perform asset tagging from CMDB to Nexpose. Responsible for dissecting vulnerability scan reports and working with different IT ops team (network, server, application, end user computing) Hands-on working with Symantec CCS (Control Compliance Suite) tool generating the MSB (Minimum Security Baseline) reports. Troubleshooting when a scan does not generate in CCS. We have managed a project to implement compliance and vulnerability using Symantec CCS. Identification of the false positive/ True positive events and act so as per the requirement.

Integration of IDS/IPS to ArcSight and analyze the logs to filter out False positives and add False negatives in to IDS/IPS rule set. Debugging the issues which are related to ArcSight ESM performance, reporting, collection of logs from various devices. Have fine-tuned several use cases and recreated the rules in ArcSight. Perform content and filter development to find data, and events of interest. Develop filters to aid in the identification of significant events. Create Queries, Use Cases, Reports, Dashboards, and Correlation Rules. Environment: Nexpose, Symantec CCS, ArcSight, Linux Security Analyst Cyber Security Team July 2017 to October 2017 Responsibilities: Worked as a Cyber Security Team member and supported the Qradar environment. Hands on with Nexpose Rapid7. Integrated Falcon Crowd Strike and few other devices to the Qradar for bringing the events. Enhancement and fine tuning of correlation rules on Qradar based on daily monitoring of logs. Monitoring of day to day system health check-up, event flow data backup, and system configuration backup. Recommended and Configure Daily and weekly and monthly reports in Qradar based on the compliance requirements. Worked on IDS/IPS using Cisco Firepower source. Configured rules, reports and dashboards in Qradar. Environment: Qradar, Nexpose Rapid7, Linux IT Security Analyst CVS Caremark - Woonsocket, RI August 2015 to June 2017 Responsibilities: Worked as a part of Security Operation Center (SOC) and was handling different components like Log Collector, Log Decoder, Concentrator, and collection from a wide variety of products distributed across categories of servers, network devices, databases and apps. Installation of connectors and integration of multi-platform devices with ArcSight ESM, develop Flex Connectors for the ArcSight unsupported devices/custom apps. Develop content for ArcSight ESM like correlation rules, dashboards, reports and filters. Creating alerts and reports as per business requirements and threat modelling with specific security control requirements. Have used Intrusion Detection and prevention (IDS/IPS), and malware investigation devices. Attending weekly client meetings in that need to discuss about on boarding and content testing results status. Created installation and configuration and test case scenarios documents for each specific device connectors. Have worked on patch management. Helped in testing of controls and the remediation of any deficiencies found. Help in developing vulnerability reports for operation teams

and process functions. Recommended security strategies based on real time threats. Environment: ArcSight, Linux, Windows. Security Analyst Georgia Pacific - Atlanta, GA January 2015 to July 2015 Responsibilities: Installed Splunk universal forwarders across various applications to collect the data. Created and configured management dashboards and reports. Created Splunk dashboards to capture the authentication breaches across applications. Have worked on Symantec anti-virus. Have extracted various fields from different types of log sources using regular expressions. Analysis of offenses created based on different device types of logs via Correlation rules. Integrate different feeds to Splunk Environment. Integration of different devices data to Splunk Environment. Environment: Symantec, Splunk. Security Analyst American Express - Boston, MA June 2014 to December 2014 Responsibilities: Configuring and testing of log generation and collection from a wide variety of products distributed across categories of servers, network devices, security devices, databases and applications. Develop and test ArcSight asset modelling, it is used to populate asset properties in Correlation rules and reports. We on-boarded 9000+ devices to ArcSight ESM for Threat detection. Monitoring and identify any suspicious security events using the ArcSight ESM console and raise a ticket in the Dbsoc portal Investigate and identify events, qualify potential security breaches, raise security incident alerts and perform technical & management escalation. Received several Spam emails from the DB users and coordinated with messaging team to block email ids. Received the Virus alert for outbound and inbound and coordinated with Antivirus team. Environment: ArcSight, Linux, Windows. Security Analyst Smartnet IT Solutions - Hyderabad, Telangana April 2012 to December 2013 Responsibilities: Maintain Qradar console, event processors, flow processors, event collectors, flow collectors to global payment environment for log collection and monitoring. Recommended and configure correlation rules and reports and dashboards in Qradar. Analysis of offences created based on different device types of logs via correlation rules. Enhancement and fine tuning of correlation rules. Environment: Qradar, Linux Education Bachelor's Additional Information Technical Skills: Security Products HP ArcSight SIEM, Splunk SIEM, IBM Qradar etc. Vulnerability Management Nexpose Rapid7, Symantec CCS Email Firewalls Barracuda Spam Filter

Web Tools Cisco Umbrella, Barracuda Web Filter  Antivirus Sophos, Ensilo  Operating Systems Linux, Windows family.

Name: Natalie Chavez

Email: alan18@example.org

Phone: +1-515-228-5876x249