Prashanth
kp671674@gmail.com
(347) 850-2640

SUMMARY

Sr. Security Engineer with over 9 years of experience on Web Application Security, Vendor Risk Management, Risk Assessment and Penetration testing. Effective communicator with interpersonal skills to collaborate across teams, stakeholders to achieve core business objectives.

SKILLS:

- Cloud Security
- Application Security
- DAST
- SAST
- Threat Modelling
- Vendor Risk Management
- Vulnerability Management
- Incident Response

EXPERIENCE:

Sr. Security Engineer
Los Angeles, CA
Frontdoor Inc/ Sept 2022 – Current

- Perform security reviews and provide insights throughout all phases of software development
- Work with IT Groups to define, develop, socialize and execute long-term application security roadmap
- Conducted web penetration testing to identify OWASP Top 10 security threats and proficient in remediating application level vulnerabilities like XSS, SQL Injection, CSRF, authentication bypass, cryptographic attacks, authentication flaws developed in different platforms like Microsoft .NET, PHP, Java, React JS, Ruby using Kiuwan (SAST), Acunetix (DAST) and triage the findings using Burpsuite
- Experience reviewing and interpreting Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Rapid 7 insight VM etc
- Collaborate with development teams to ensure secure development standards and secure coding best practices are followed

- Worked closely with the devops team in integrating Static Code Analysis tools like Checkmarx and Veracode into the CI/CD pipeline using Jenkins as part of the Secure SDLC process
- Provided security recommendations as a subject matter expert for development teams during all phases of critical systems such as Authentication, development and even language specific implementations of certain Caching and more.
- Developed and delivered training around secure development lifecycle for different teams and secure coding practices by implementing standards for languages and their dependencies.
- Threat modelled web applications, mainly structured as cloud native and microservice oriented and worked with the process in their workflow to enhance the development teams throughout the agile SDLC to integrate deployment confidence and application resilience.
- Building and Deploying Malware Reverse Engineering Lab setup with Cuckoo and Elastic Search.
- Analyzing Malware Files with static and dynamic code analysis to write detections and YARA rules.
- Automation Scripting with REST API, Terraform, AWS Lambda
- Performing Incident Response and Forensic Investigations for Endpoints and AWS Instances.
- Deploying and on boarding Data for SIEM Tools like Splunk, Elastic Search, Alienvault and Sumologic.
- Utilized MS Project to track earned value management/EVM

Sr. Application Security Engineer
San Diego, CA
Jack in the Box/ Mar 2020 – Aug 2022

- Built the Application Security program from ground up and established standards, policies,operating procedures around design and development of secure code
- Conducted web application penetration testing to identify OWASP Top 10 security threats using SAST and DAST tools like Veracode, Rapid 7 Insight VM
- Built and automated secure SDLC controls and best practices in both waterfall and agile, CI/CD- focused development processes
  Performed daily monitoring of the Intrusion Detection Systems (IDS) console for activealerts and determined priority of response
- Experience in network centric analysis utilizing a variety of tools and techniques such as Network Security Monitoring, log analysis
- Prepared detailed documentary / technical report to the development team which consists of vulnerability lists, their causes and mitigation or suggestions to over each of them and steps as to where the flaw was identified. Using tools like Tenable Nessus,

Rapid7 Insight VM
Improve the security posture of information systems and network by detecting threats and vulnerabilities in target systems, and applications by conducting systems, network testing using Rapid 7 Insight VM

- Demonstrated project management capability including earned value management (EVM)
- Experience working with cloud-based data storage architectures and the controls commonly used to secure those environments, such as encryption, tokenization, data masking, data lifecycle management

Strong experience with AWS services such as GuardDuty, Key Management, Inspector, S3, Cloud Formation, CloudWatch, Cloudtrail, AWS Config, EC2, VPC, IAM

- Build servers using AWS, importing volumes, launching EC2, RDS, creating security groups, auto-scaling, load balancers (ELBs) in the defined virtual private connection

Expertise in automation tools like Git, Subversion, Maven, Jenkins, Chef, Puppet, Ansible, Terraform, Docker

- Have built Docker images and written Docker files which can be used to automate all developer tasks
- Review alerts from managed services providers, perform log analysis/correlation, determine malicious software behavior, vet out False Positives, assist in remediating system misconfigurations, tracking system state changes and other information across multiple systems. Leverage outputs to support forensic reconstruction as needed.
- Detect, respond, mitigate, and report on cyber threats/incidents that may impact the environment. Utilize analytics to identify potential threats.
- Collaborate with technical leads: Engineering/Operations, Service Desk, Applications, business stakeholders and external partners on matters related to security monitoring.
- Secured on-premises and SaaS web applications with two factor/ multifactor authentication (MFA)
- Configured SSO and MFA for Amazon Web Services (AWS) with IDP
- Building out the strategy and manage forward-looking security capabilities and resources for Data
- Protection, Identity and Access Management, Multifactor Authentication, Vulnerability Management, and Asset Management

Security Engineer
Los Angeles, CA
Smartmatic/ Mar 2019 to Feb 2020

- Develop new security solutions/tools to prevent security vulnerabilities and assist in addressing existing security problems
- Experience reviewing and interpreting Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burpsuite

- Continuous monitoring and interpretation of threats through use of intrusion detection systems, firewalls and other boundary protection devices, and any security incident management products deployed.
- Coordination of incident response activities, including written and verbal communication with other IT groups and IT management
- Work through prioritized vulnerabilities for patch remediation with respective asset owners
- Strong experience with cloud security strategy, cloud provider ecosystems (Amazon AWS/ Microsoft Azure) in vendor integration, platform integration and monitoring
- Worked with Ansible (automation tool) to automate the process of deploying/testing the new build in each environment, setting up a new node and configuring machines/servers
- Developed custom Jenkins jobs/pipelines that contained Bash shell scripts utilizing the AWS CLI to automate infrastructure provisioning
- Perform static/dynamic code testing, manual code inspection, threat modeling, design reviews and penetration testing of internal web applications and external partner applications to identify vulnerabilities and security defects.
- Building Dashboards, Apps and Alerts in Splunk
- Performing Threat Hunting and Creating Custom Detections in EDR solutions.
- Building Terraform Templates for Lambda and Docker Deployments
- Creating Automated Cloud Forensics environment deployment to reduce Incident handling time
- Building and Securing Docker Containers with Terraform and AWS Fargate
- Gathering Evidence and Assisting Organization for PCI DSS, SOC2 Audits

Information Security Engineer
Henderson, Nevada
Barrick Gold Corporation/ May 2018 to Mar 2019

- Develop secure code practices and provide hands-on training to developers and quality engineers
- Conducted web application penetration testing to identify OWASP Top 10 security threats using SAST and DAST tools like Veracode, Rapid 7 Insight VM
- Built and automated secure SDLC controls and best practices in both waterfall and agile, CI/CD- focused development processes
- Performed daily monitoring of the Intrusion Detection Systems (IDS) console for active alerts and determined priority of response
- Also investigated and analyzed logs and events on any incidents or security breaches to identify root cause and used tools like NMAP and Nessus and Wireshark for network scanning
- Classify and prioritize the risk of all vulnerabilities taking into consideration mitigating factors and impacts of internal and external threats

- Conducted security awareness training for employees on spam emails and phishing attempts using a module called WOMBAT specifically designed for this purpose and provide tactical response for phishing attempts within 24 hours
- Burp Suite for web application penetration testing.
- Vulnerability Management and Dynamic Application Security Testing (DAST) using Nexpose/Veracode. - Network/Infrastructure penetration testing on USC network to check for potential vulnerabilities and bugs.
- Validate vulnerability reports generated by scanners for false positives and patch with required remediation.
- Documentation of "External Penetration Testing" and "Bug Bounty Recon Methodology" runbooks.

Associate Application Security Engineer
Secure App Technologies Feb 2017 to May 2018

- Provided security support and evaluation to development teams to integrate information assurance (security throughout the System Life Cycle Development of major and minor applications
- Training the development team on vulnerabilities, review issues, ease of exploitation, impact, security requirements and remedies for individual issues
- Create Vulnerability Assessment report detailing exposures that were identified, rate the severity of the system, and suggestions to mitigate any exposures and testing known vulnerabilities
- Created and configured security use cases for Network and User behavior analytics using resources like NetFlow, Checkpoint, Windows Security, Tanium, CloudTrail and more
- Monitored, investigated, analyzed, and documented the security incidents to find the true positives and false positive cases using Splunk, MySQL and Crate
- Provided metrics for the designed Security Use cases
- Security research of the current threats and attacks to build User and Network behavior analytics use cases
- Developed automations to perform day-to-day operations using bash
- Interacted with various customer technical leads during Incident response investigation

- Developed prototypes of system designs and working with database, operations, technical support, and other IT areas as throughout development and implementation processes
- Performed manual and automated vulnerability assessments of the AWS VPC

Cybersecurity Analyst
Chennai, India
Byte to Bit Technologies/ Jun 2012 to Aug 2015

- Day-to-day operational tasks related to the ongoing support of the Security Operations

- Responsible for the tracking and assignment of tickets/events to Security Operations Team, maintenance & monitoring of security tools
- Detection and response to security incidents that occur within the company and have conducted assessments that include social media monitoring, malware vetting and loganalysis
- Network recon and network mapping: Analyzed the network configurations using the Solarwinds network monitoring tool and gathered the network topology data of global locations
- Segregated the workstations & servers to schedule the NESSUS scans using the network topology information
- Monitored emails and threat alerts of end-point systems using IronPort and Sophos respectively
- Reported and helped the team with Incident Response investigation
- Provided the ISAT documentation to train the employees using digital signage
- Identified and tested CSRF vulnerabilities using Burpsuite and recommended mitigation measures

EDUCATION AND TRAINING

Master of Science: Information Security Wilmington University Dec 2016
New Castle, Delaware

ACTIVITIES AND HONORS

Meditation facilitator and a part time volunteer with a non-profit working with university students to create awareness about mental health.