AWS Security and Compliance Analyst

Over 10 years of industry experience in software life cycle, including system analysis, designs, development, testing and implementation which includes, 6 years in implementing cyber security, policies, rules and standards including incident response monitoring and Threat analysis and risk mitigation on endpoints networks and applications with + in Cloud Services AWS Cloud Services(EC2, S3, IAM, VPC, Cloud Formation, Dynamodb,) Azure and Devops tools (Jenkins).

Certified Ethical Hacker CEH e-council.

- Good exposure to System/Network Analysis, Intrusion Detection, and Malware Analysis
- Involved in managing documentation to support IT security processes
- Provide root cause analysis and remediation techniques for management regarding security incidents and governance documents
- SIEM Facility(Q radar), vulnerability management (Rapid7-insight vm Nexpose), Threat Management (Fire Eye) And Email Security Barracuda, solar winds (NPM, SAM)
- Experienced with Vulnerability Scanning tools like Nessus, Rapid7 and Qualys
- Implemented and Maintained SIEM infrastructure using Q radar and Splunk
- Member of Sec-Ops team for Incident Response plans and layouts
- Requirement gathering and performing functional and detailed design analysis, and responsible for developing guidelines, standards and implementations
- Working with Security Operations Center (SOC) to find the existing log gaps and provide a better data analysis to increase the overall Security coverage
- Performed/Assisted in installation, configuration, troubleshooting and maintenance of SIEM Agents, Log Managers/Collectors, SIEM Central Managers/Aggregators
- Created custom reports and dashboards for various IT Teams that utilize SIEM
- Worked with various IT Teams and created User Roles and Accounts specific to their Job Functions
- Defining security standards and analyzing architectural security between Base Architecture on-premises and Target Architecture in cloud.
- Solid hands-on experience on designing AWS cloud architecture and over 4 Years of experience on designing the frameworks.

- Solid hands-on experience in provisioning EC2, EBS, S3, Elastic Load Balancer, Auto Scaling, ECS, CloudWatch alarms., Cloud formation templates, Virtual Private Cloud (VPC), IAM, implementing Security of data in transit and at rest.

- Implementing Encryption at rest, in S3 bucket, object-based permission ACL, role based permission, IAM policies was component access restrictions.

- Good experience on Amazon AWS IAM Service: IAM Policies, Roles, Users, Groups, AWS Access Keys and MFA.

- Configured AWS IAM and Security Group in Public and Private Subnets in VPC. Architected, Designed and Developed the Backup and Archiving, Disaster Recovery in AWS Cloud.

- Experienced working with methodologies like Agile SCRUM.

- Proficiency in developing Cloud Security policies and strategies in par with the organization's compliance structure. Providing Risk Management and mitigation recommendations for projects in organization.

- Good knowledge of threats analysis and remediation efforts about Intrusion prevention and penetrations

- Provide root cause analysis and remediation techniques for management regarding security incidents and governance documents
- Involved in enhancing the stature of the project by initiatives like Threat Modeling, awareness security

- Maintain proper auditing standards of SSAE 16, ISAE 16, SAS70, AT101

- Good knowledge in compliance requirements and understanding of SERIES standards based on (NVD) National vulnerability databases.

- Good knowledge in writing firewalls rules, reviewing and Database Activity Monitoring (DAM)

- Good Understand of OWSAP Top 10 and SANS vulnerabilities

- Experience into End point security, Application Security and Change Management.
- Good knowledge on networking and wireless concepts like DNS, Routers, Gateways, Switches, TCP/IP protocols and subnets.

Work Experience

SECURITY ENGINEER |CYBER SECURITY ANALYST | CLOUD SECURITY -
Cognizant Dallas TX
From January 2018 - Till date

- Launching Amazon EC2 Cloud Instances using Amazon Web Services (Linux) and Configuring launched instances with respect to specific applications.
- Perform S3 buckets creating, policies and the IAM rule based polices
- Designed highly scalable and fault tolerant, highly available and secured, distributed infrastructure (IAAS) using EC2 instances, EBS, S3, RDS, ELB, Auto Scaling, Lambda, Redshift, DynamoDB etc. in AWS Cloud
- Interacting with clients to capture requirements.
- Gathered user requirement and performing functional and detailed design analysis.
- Designing and implementing both the front-end and back-end systems that run on AWS on par with organization compliance and security policies.
- Provided Migration plan and strategy for cloud, and strategy to migrate infrastructure and data from On-premises data center to AWS Cloud
- Configuring DNS (Route53), ELB, general networking principles, firewalls, route tables and route propagations.
- Create and maintain SSL Security certificate management for enterprise, maintaining certificates across multiple SSL-providers, and integrating certificates into products such as nix, apache, tomcat, AWS -ELB.
- Build servers using AWS, importing volumes, launching EC2, RDS, creating security groups, auto-scaling, lad balancers (ELBs) in the defined virtual private connection.
- Defined Access policies and access groups among internal and also customers
- Designed Robust Environment for connectivity between On-Premises and Cloud for existing on-premises Apps
- Implemented monitoring process of cloud environment and notification system using cloud watch and SNS.
- Designed Successful Data Migration approach using AWS DMS and Scheme Conversion tool and policy for infrastructure migration to Cloud environment
- Creating and presenting MS Power point presentation for Technical and non-Technical management team.
- Followed Agile Methodology and scrum for implementation.

- Design a Continuous Delivery platform and implementation to provide a complete working Continuous Delivery solution using industry-standard open source tools such as Jenkins, Puppet, and Chef etc.

- Solid experience in designing data retention strategy along with automatic backup plan using SNS and scheduler

- Designing and creating highly scalable, highly available, fault tolerant, highly secured, distributed infrastructure (IAAS) using AWS EC2 instances, EBS Snapshot, S3, Elastic Load Balancer, Auto Scaling, Cloud Watch, Cloud Formation, RDS, KMS, Lambda, Redshift, SNS etc.

SECURITY ENGINEER CONSULTANT

- Performed log analysis, event management, reporting and threat analysis using McAfee ESM and Splunk for 15 clients with over 28,000 devices Leading a Security operation center (SOC) team of 15 people

- Performing Forensic investigations upon the request from Management and Internal Auditing Team

- Part of the Blue Team to identify the vulnerabilities and have a defense mechanism in place.
- Learned and helped Security team with Log collections, analysis, and forensic activities.
- Investigating logs and payloads for server crashes/core dumps, DDoS attacks, SQL/XSS, SPAM, etc.

- Effective Data Loss Prevention and Endpoint detection mechanism, using Virtru and Trend solutions, to protect data at rest, in motion and in transition

- Performed daily operation real-time monitoring, analysis and resolution of security events multiple sources including, but not limited to events from security information Monitoring tools

- Carry out network and host-based intrusion detection on client network and endpoints, content filtering solutions, firewall logs and system log matching existing SLA.

- Create and optimize alerting, reporting and advanced dashboards for SecureVue EIQ and McAfee Enterprise Security Manager (ESM) tool and other reporting tool

- Incident reporting and Risk monitoring with Sourcefire, Configuration /deploying and troubleshooting of Firewalls – Palo Alto, Check Point, Cisco ASA, Fortigate, Sophos, WatchGuard.
- Design , planning , leading and developing cyber security environment (Advance Threat Detection and IPS/IDS and Proficient with Cisco Identity service engine (ISE)

- Ensured organizational compliance by implementing Industrial standard frameworks Executed benchmarks, maintained security policies, incident response and business continuity plans

- Troubleshoot and fine tune the SecureVue EIQ and McAfee Enterprise Security Manager (ESM) deployment to ensure utmost availability and performance; This includes analyzing errors and system information, executing system utilities developing and implementing potential automation and performing configuration modifications for resolution

- Analyzing network traffic using a SIEM. Using intelligence tools, applying attribution to IOCs or actor behaviors.

- Utilizing IBM QRadar, ThreatQ and resources to determine if systems are vulnerable.
- Proactively hunting for and research potential malicious activity and incidents across multiple platforms using advanced threat network and host-based/open source tools

- Use both internal and external threat intelligence to build indicators of compromise into monitoring tools, be able to integrate these tools with one another to provide data enrichment.
- Actively preparing All Hands intelligence Meeting sharing the information with the all the Security Operations Center team folks.

- Collecting Intelligence feeds from paid sources like FireEye, Crowdstrike, Proofpoint, Palo Alto, Recorded Future, Secureworks, opensource platforms like Alienvault.

- Maintain and employ a strong understanding of advanced threats, continuous vulnerability assessment, response and mitigation strategies used in cybersecurity operations

- Provide support in the detection, incidence response, mitigation and reporting of real or potential cyber threats to the environment analyzing false positives and be able to assist in the automation of these processes

- Maintaining a strong understanding of advanced threats, continuous vulnerability assessment
- Providing resolution plans for system and network issues.

- Using extensive TCP/IP networking skills to perform network analysis to isolate, diagnose potential threats, anomalous network behavior and Preparing the reports like Actionable intelligence reports, weekly.

- Troubleshoot and researched security incidents based on QRadar Network Flow Log Activity.
- Analysis of multiple log sources including firewalls, routers, switches, web servers and multiple networking devices.

- Installing and configuring Qualys in premises and on cloud environment. Responsible for performing vulnerability assessment on critical systems using Qualys.Configured and scheduled Qualys Scanner in QRadar to perform scan on regular intervals

- Collaborate with team members in tuning SIEM applications to establish a baseline for network activity and rule out false positive events.

- Integration of different devices/applications/databases/ operating systems with Qradar SIEM
- Monitor security alerts from IBM Qradar and report any issues to the concerned team.

- Monitor and analyze data feeds of events and logs from firewalls, routers, and other network devices or host systems for security violations and identify vulnerabilities.

- Implemented and maintained McAfee Endpoint Encryption system to protect computers.
- Advanced threat detection, Antivirus, MacAfee IDS/IPS rule sets and signature creation, packet analysis.

- Perform vulnerability scanning and assist with compliance auditing to ensure customer networks conform to all relevant compliance standards, including PCI-DSS, HIPAA and Sarbanes-Oxley

- Manages PCI Compliance Program for organization protecting cardholder data and executing the PCI-DSS Program Life Cycle.

- Performed day-to-day administration of McAfee EPO 5.1 for maintenance of system policies, container maintenance, coordination of system maintenance and client upgrades for desktop environment
- Responsible for assisting various sites with troubleshooting and integrating all aspects of the ePO5.3 suite to include HIPS, Asset Baseline Monitor, AV, Rogue System detection, Policy Auditor.

Application Security

- Recommended remediation actions for the security vulnerabilities.
- Familiarity with tools like Nmap, Kali Linux, BurpSuite, Owasp zap, Qualys, Acunetix, Wireshark etc.

- Performed web application vulnerability scans (e.g., AppScan, web inspect, Accunetix, Burpsuite Pro, etc) knowledge of the OWASP, WASC security Standards and detailed knowledge of common web application attack vectors such as SQL injection, CSRF, XSS, Session Management issues, Direct Object reference, Click jacking, buffer overflows, etc.

- Determined hardware and software requirements; acquired equipment; established user
- Conducted Dynamic security Scans, Manual validations/Pen Testing, and other QA activities. Pen Testing and Ethical hacking activities using tools like OWASP ZAP and web inspect.

- Worked with DevOps teams to automate security scanning into the build process.

- Reviewed security vulnerability reports for application and databases, analyzed and worked extensively with the development teams for the implementation of mitigating controls.
- Conducting Vulnerability Assessments and Penetration Testing on Web Application, Mobile Application/devices, and Infrastructure. detect and report the security issues in various environments.

- Write comprehensive reports including assessment-based findings, outcomes and propositions for further system security enhancement.

- Understanding of tools like HP Fortify, IBM Appscan, Webinspect, Nmap, Nessus. Burp Suite, Nessus Automatic Scanner
- Analyzed the Exploited systems with vulnerabilities using Metasploit framework.

- Static and dynamic scanning of various application using HP Fortify and HP Webinspect, Identify false positives and reports it to soc
- Identify critical, High, Medium, Low vulnerabilities in application based on OWASP Top 10.

- Real time experience in DOS, DDOS, SQL Injection protection, XSS protection, script injection and major hacking protection techniques.
- Integrating security in SDLC by following techniques like Threat Modeling, Risk Management, Logging, Penetration Testing, etc

AWS CLOUD ENGINEER | CLOUD SECURITY

- Creating new AWS accounts under the Master Pair
- Configured SSO on AWS accounts
- Creating Predefined AWS Roles for respective users to assume
- Roles for EC2, ECS, ES, Lambda, S3, IAM Pass Role, DynamoDB
- S3 Roles for Bidirectional replication
- Configuration and administration of Splunk for cloudWatch and cloud Trail logs
- Configured SSO for Splunk
- Creating users with requested access under Splunk
- Documenting all configuration done on cloud
- Brought up Hybrid network by configuring IPSEC VPN Tunnel and Direct Connect
- Configured AWS Sandbox account (shared account) for short term development and testing
- Configured VPC Isolation policy under AWS Sandbox account for security and Configured Billing alerts
- Security Risk and Maturity Assessments, including PCI DSS, NIST and FFEIC working directly with regulators and senior leadership in
- various organizations providing leadership, oversight and prioritization of remediation efforts, creating value by verifying proper implementation of information security controls, identifying key trends, determining root cause, analyzing data, audit reports, network penetration test results, application security assessments, regulatory exams, and delivering tailored metrics and reporting.
- Hands-on experience developing, maintaining and updating strategic risk and maturity assessment roadmaps, performing
- Third-party security evaluations and risk assessments in adherence to industry frameworks (NIST, ISO, PCI DSS, COBIT) and regulatory compliance (SOX, GLBA, GDPR).
- As a Solution Architect , responsible for business engagement, customer requirements, business communications, team management & delivery.
- Configured IAM roles for user level access security
- Configured AWS security groups and Network ACLs policies for additional layer of security
- Configured VPC landscape for 4 different environment - Dev, Testing, Prod Test and Production As per the requirement configured AWS services - S3,Auto Scaling ,CloudWatch ,CloudTrial

SECURITY ENGINEER
Accenture Dallas TX
From 2012 till 2018

Security Consultant

- Developed and refined procedures for Monitoring, Detecting, Reporting, Logging and Investigating Information security generated by network hardware and applications through SIEM tools such as HP ArcSight.

- Used remediation techniques for all collected vulnerabilities and if it is very high severe vulnerability then ticket escalate to the higher authority

- Responsibility for the planning and controlled execution of releases into the managed environment

- Performed Vulnerability scanning on web applications and databases to identify security threats and vulnerabilities.

- Monitor the security of critical systems (e.g., e-mail servers, database servers, web servers, etc) and changes to highly sensitive computer security controls to ensure appropriate system administrative actions, investigate and report on noted irregularities.

- Performed Risk Assessment and drive the closures of identified Risk.
- Vulnerability Management: Configured Qualys, Nessus Guard Tool for Vulnerability Analysis of Devices and Applications. Monitored them constantly through the dashboard by running the reports all the time.
- Conducted analysis, Cyber threats, the discovery of IT vulnerabilities, monitoring for cyber intrusions, troubleshoot and response to security incidents detected from HP ArcSight and related SIEM. IDS/IPS, and other security applications.

- Architected Splunk Cloud SIEM deployment for Enterprise level covering 80K+ Endpoints - with Billion Logs/Day

- Worked with various log source types' integration to Splunk and Built Event Types, Field Extractions, Data Models etc Working on building the on-premise infrastructure to support the Splunk Cloud SIEM

- Working with security Operations Center (SOC) to find the existing log gaps and provide a better data analysis to increase the overall security coverage

- Implementing SOC Rules for all the SIEM platforms which includes Anti-Virus like Symantec/McAfee, Authentication for Windows/Linux, Malware, Database, Firewall, IPS, Server, WLAN, Web Proxy etc. that reinforce the organization from different attacks and reduce the overall security risk Worked with Security Operations Centre (SOC) to fine-tune the False-Positives from the existing SIEM Rules

- Created custom reports and dashboards for various IT Teams that utilize SIEM

- Managed the Database Activity Monitor Tool as a Backup-Owner/Administrator

- Performed/Assisted in installation, configuration, troubleshooting and maintenance of SIEM Agents, Log Managers/Collectors, SIEM Central Managers/Aggregators

- Develop, implement and update, new and existing FIM Policies working with various IT Teams and created User Roles and Accounts specific to their Job Functions.

- Create and optimize alerting, reporting and advanced dashboards for SecureVue EIQ and McAfee Enterprise Security Manager (ESM) tool and other reporting tools
- Incident reporting and Risk monitoring with Sourcefire, ESM.
- Configuration /deploying and troubleshooting of Firewalls – Palo Alto, Check Point, Cisco ASA, Fortigate, Sophos, WatchGuard
- Solid understanding of security principles and technologies (SIEM tools e.g. ESM, Q Radar and SPLUNK)
- Proficient with Cisco Identity service engine (ISE).
- Identity and access – 802.1x, Radius, PKI, 2-factor authentication and content filtering.
- Responsible for monitoring, tracking and analyzing records and incidents to ensure protection from any potential leaks or malicious activity
- Configuring/Troubleshooting Network Security – IPsec, VPN, AAA Architecture, TACACS+, RADIUS
- Knowledge of internet protocols (e.g. TCP/IP, BGP, OSPF, TACACS, IPSEC SNMP,SYSLOG)
- Vulnerability assessment and scanning (Nessus and Nexpose)

- Cisco ISE implementation, configuration and optimization on different versions 2.1, 2.2 of several patches.

AWS
Responsibilities:

- Hands on experience in Amazon Web Services AWS provisioning and good knowledge of AWS services like EC2, Auto scaling, Elastic Load-balancers, Elastic Container service (Docker containers), S3, Elastic Beanstalk, Cloud Front, Elastic file system, VPC, Route 53, Cloud Watch, Cloud Formation, IAM.

- Involved in designing and deploying a large applications utilizing almost all of the AWS stack (Including EC2, Route53, S3, RDS, Dynamo DB, SNS, SQS, IAM) focusing on high-availability, fault tolerance, and auto-scaling in AWS Cloud Formation.

- Managed multiple AWS accounts with multiple VPC's for both production and non-prod where primary objectives included automation, build out, integration and cost control.

- Developed Cloud Formation scripts to automate entire CD pipeline.

- Created and managed multiple Instances of Apache Tomcat and deployed several test applications in those instances in QA environment.

- Configured a VPC and provisioned EC2 instances, EBS in different availability zones.

- Implemented and maintained the monitoring and alerting of production and corporate servers/storage using AWS Cloud Watch.

- Setup and build AWS infrastructure various resources, VPC EC2, S3, IAM, EBS, Security Group, Auto Scaling and RDS in Cloud Formation JSON templates.

- Creating Cloud Watch alerts for instances and using them in Auto Scaling launch configurations.

- Implementing good security compliance measures with MFA and authentication and Authorization with IAM roles

- Backing up the instances by taking snapshots of the required servers regularly.

- Setting up and administering DNS system in AWS using Route53.

- Written Several Chef cookbooks from scratch consisting of recipes that can Provision several pre-prod environments consisting of WebLogic domain creation, Deployment automation, instance mirroring, and several proprietary middleware installations.

Admin Support
Mutual Benefits Assurance
2009 -2012

CERTIFICATION
CCNA certification R&S
CEH Certified Ethical Hacker