C:\Users\Shahnawaz\AppData\Roaming\Skype\adam.softnice\media_messaging\media_cache_v3\^02DAF71B621501F2AAC48F5ECF65B22AA61BEEB31E0B90464B^pimgpsh_fullsize_distr.png

|  |  |
| --- | --- |
|  |  |

**Information Security Engineer**

Name: Anil Kumar Dirishala

Contact :[347-762-6896](tel:(347)%20762-6896)

Email :[adirishala@gmail.com](mailto:adirishala@gmail.com)

Experienced Information Security Engineer with over 5+ years of experience in information system security, engineering, and management of cyber security. This includes, but not limited to IP Networks, Network Intrusion Detection and Active Directory.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Professional Abridgement**

* Expert Level Knowledge about TCP/IP and OSI models.
* Logging and monitoring infrastructure with Splunk.
* Involved in troubleshooting of DNS, DHCP and other IP conflict problems
* Analysed Web traffic and inspected email contents for potential malware and infection.
* Knowledge base and familiarity with the latest cutting-edge technologies, including firewalls, VPN, IDS,  IPS, DMZ, encryption, IPsec, proxy services, Site to Site VPN tunnels, MPLS/VPN, SSL/VPN.
* Experience on vulnerability assessment and penetration testing using various tools like Burp Suite, OWASP ZAP Proxy, Nmap, Nessus, Rapid 7, Kali Linux and Metasploit.
* Worked on FTP, HTTP, SSL, DNS, DHCP servers in windows server-client environment with resource allocation to desired Virtual LANs of network.
* Worked on the migration to new Checkpoint R77 Firewalls on GAIA from CISCO PIX Firewalls
* Supervising the administration of systems and servers related network to ensure availability of services to authorized users.
* Experience with Firewall Administration, Rule Analysis, Rule Modification.
* Define and implementing Unix operating system strategy with application installation and configuration.
* Experience in Checkpoint Firewall on SPLAT and VPN technologies, Stateful inspection, and Global rule base, address spoofing.
* Utilized Security Information and Event Management (SIEM), Intrusion Detection & Prevention (IDS / IPS), Data Leakage Prevention (DLP)
* Experience in Splunk Development, Configuration and Administration.
* Engineered Splunk to build, configure and maintain heterogeneous environments and in-depth knowledge of log analysis generated by various systems including security products.
* Troubleshooting and resolve the Splunk - Performance, Log Monitoring Issues; Role Mapping, Dashboard creation, Data models etc.
* Experience in applying PKI technology to business systems.
* Architected new deployments of QRadar SEIM; including required hardware and EPS sizing with optimal licensing.
* Deployed custom configurations of the QRadar appliance via development of backend SQL queries for custom reporting and logging.

**Skills:**

* **Protocols** : NAT, TCP/IP, UDP, RIP, EIGRP, OSPF, VTP, VLAN, SSL, VPN, HTTP, HTTPS, FTP, DNS, ICMP
* **Switches** : Cisco Catalyst VSS 1440 / 6500, 4500, 3750, 2950, 3500XL
* **Routers** : Cisco Routers ASR 7600, 7200, 3800, 3600, 2800, 2600, 2500 , 1800
* **Languages**: Java, MySQL, python, JavaScript, Linux.
* **NetworkManagement**: Wire shark, TCP Dump, Net Flow, SNMP, Netcool.
* **OperatingSystems** : Windows XP/7/8, Windows Server 2000/2003/2008, Solaris UNIX
* **Security Tools**: Splunk, IBM QRadar, HP ArcSight, Nessus, OpenVas, Kali Linux, Rapid 7, DVWA, Metasploitable2, BlueCoat, Volatility.
* **PenTest Tools:** Metasploit, NMAP, Wireshark and Kali
* **Security Software:** Nessus, Ethereal, NMap, Metasploit, Snort, BASE
* **Firewall**: Cisco ASA, Fortinet, Juniper, Checkpoint.
* **IT Security/ Frameworks**: IDS/IPS, Malware analysis, Logging and Monitoring, Vulnerability Management, Application and Infrastructure security, Reporting and Documentation, Digital forensics, Ethical Hacking, Penetration Testing, SDLC, ITILv3.

**Certification and Education**

Master of Science in Cyber Security

Diploma in Information Assurance and Security (Level 7)

**Apple Inc. Sunnyvale, CA (Dec 2016 - Present)**

**Information Security Engineer**

* Experience building firewalls, mainframes, and UNIX based platforms at the data center and implementing the initial policies, configuring NAT, Routing etc.
* Developed python scripts to generate custom reports and FTP/Email.
* Deployed and maintained IS-IS on Cisco and Juniper routers.
* Application administration for Qradar, Splunk and Tanium.
* Responsible design, deployment operation of a Security Incident and Event Management solution based on Splunk.
* Log analysis and advisories to different customers through RSA envision SIEM.
* Experience in security for the following platforms: Windows physical and virtual desktops and laptops, UNIX / Linux Servers, Windows servers, Database as well as RSA (EMC), McAfee (Intel), FireEye, Symantec endpoint security tools and good knowledge of SAN technology.
* Deploy Tanium to support security operations in classified and unclassified environments within Department of Defense (DoD) enterprise network.
* Perform patch management to workstations and servers using the Tanium application to meet specific patching timelines.
* Utilized the Blue Coat Proxy, SIEM, SOC, Tuffin, IPS/IDS.
* Initiated global projects deploying zScaler, Symantec Endpoint Encryption, Qualys and SourceFire NIDs.
* Create and maintain high-quality documentation of all relevant specifications, systems, and procedures.
* Supporting the activities of UNIX vulnerability by identifying, prioritizing and eradicating risks in UNIX environments.
* Repaired and diagnosed UNIX hardware and application software.
* Develop data cleansing, retrieval, migration tools (ETL) using python.
* Maintained 15 Juniper 6611/4610/2600 Remote Access Pulse Secure MAG firewalls.
* Worked in Data center environment with Cisco UCS 6200 interconnects Cisco UCS B-series Blades and Cisco UCS 5100 series blade server chassis and implemented RAC mounted servers.
* Operational experience with Blue Coat technology (Proxy SG, Director/Management Center, Proxy AV/Content Analysis System (CAS), WebPulse, Data Leak Prevention (DLP), Authentication and Authorization Agent (BCAAA) or equivalent from another enterprise-class proxy vendor (e.g., Cisco, Forcepoint (formerly Raytheon Websense), or Intel Security (McAfee))
* Experience in managing Active Directory Domain Controllers, DNS and DHCP Servers.
* Utilizing ArcSight Smart Connectors, Logger appliances and HBSS server log analysis to verify proper SIEM security event flow.
* Performed mobile security assessments.
* Created and managed use cases, analyze correlated traffic, created and monitor channels, create and send reports, collected detailed evidence to support cases with SIEM HP Arcsight Application Worked with SIEM tools such as IBM QRadar to get real-time analysis of security alerts generated by network hardware and applications.
* Tested application and general IT control for SOX and FSA clients. Performed operational control testing for SSAE16 clients.
* Extract the logs, perform real time log analysis using SIEM technologies and Forensics Analysis of logs as per the request.
* Followed PCI standards for creating policies.

**Pitney Bowes** **,Shelton, CT(Oct 2015- Nov 2016)**

**Security Analyst**

* Managed several security technologies including McAfee Endpoint Security (HBSS), Nessus Vulnerability Scanner (ACAS), Tanium ESSM, AirTight, SCCM, Splunk, and other security tools managed by the enterprise security team.
* Experienced in Implementing & managing Symantec Data Loss Prevention.
* Implemented long term security measures, patches and honeypots.
* Experienced in creating, testing and implementing DLP Policy/Rules to ensure client data confidentiality.
* Experience in security for the following platforms: Windows physical and virtual desktops and laptops, UNIX / Linux Servers, Windows servers, Database as well as RSA (EMC), McAfee (Intel), FireEye, Symantec endpoint security tools and good knowledge of SAN technology.
* Responsible for Data Loss Incident investigation and Remediation.
* Proficient in writing arcsight queries, dashboards and reports for DLP Incident metrics.
* Installation, configuration and set up of arcsight and relevant components.
* Customizing correlation searches, alerts, reports and dashboards using Arcsight loggers and Connectors.
* Working with Arcsight support team for various arcsight issues and licenses.
* Familiar with IDM solutions such as Provisioning, Review, SoD (Segregation of Duties) and PDM (Profile Data Mapping).
* Issue, revoke, renew and recover certificates for the PKI office in compliance.
* Experience in packet analysis and packet capture using Wireshark.
* Daily responsibilities included design, implementation, support and administration of multiple security products running CheckPoint Provider-1, SourceFire.
* Monitor and investigate security incidents and alerts with arcsight, FireEye, Palo Alto, SourceFire and McAfee EPO.
* Built custom Tanium sensors to fill the gaps that where left by our other data collection tools.
* Analyze prevention from the invasions through the malware detection and removal.
* Threat Hunting with Splunk, Qradar, Tanium and RSA Security Analytics.
* Application administration for Qradar, Splunk and Tanium.
* Experience working with Network monitoring using tools like Netflow Analyzer and Netcool for troubleshooting issues.
* Implementing monitoring solution to gather data on ISP utilization and Netflow management.
* Extensive experience in business process engineering and software development life cycle, including analysis, design, development, testing and implementation of software applications.
* Experience in configuring the security policies using Juniper NetScreen.
* Extensive knowledge in Business Analysis, PKI, SSO, Kerberos, TCP/IP, DNS, VPNs and Symantec DLP
* One (1) Arcsight ESM Installation Upgrade and Migration from ESM 6.0 to 6.9p1
* Four (4) Arcsight Express Installations and Migrations
* Arcsight ESM software / Arcsight Express appliance installation and configuration
* Develop systems that assist the organization to secure the CIA categorizing and selection ofcontrols using NIST.
* Followed AAA security principles for securing the information.
* Performed DDOS mitigation to avoid data theft and downtime.

**Hexagon Solutions , India (Jan 2012- July 2015)**

**Security Analyst**

* Performed Computer Security Incident Response activities for a large organization, coordinates with other government agencies to record and report incidents
* Monitored and analysed Intrusion Detection Systems (IDS) to identify security issues for remediation
* Recognized potential, successful, and unsuccessful intrusion attempts and compromises thorough reviews and analyses of relevant event detail and summary information
* Evaluated firewall change requests and assess organizational risk.
* Provide guidelines for implementing secure systems to customers or installation teams.
* Assisted with implementation of counter-measures or mitigating controls.
* Ensured the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices.
* Performed periodic and on-demand system audits and vulnerability assessments, including user accounts, application access, file system and external Web integrity scans to determine compliance.
* Design the Web listeners and firewall policy rules on reverse proxy to allow the Internet users to access the Internal servers/ resources through Internet.