**Kipley A. Keene**

236 Muses Mill CT Holly Springs, NC 27540 Cell :(919) 332-1178 ,kipkeene718@gmail.com

**SUMMARY:** Information Technology specialist with over ten years of experience. Managed helpdesk tickets for desktop and networking problems. Maintained LAN servers for upgrades and break fix repairs. Maintained ESXi server virtualization platform, HBSS server and Performed weekly backups of critical information using backup applications for storage. Reviewed changed control procedures for onsite hardware. Performed endpoint system hardening with HBSS, patching and documented change processes for vulnerability fixes. Daily assignments include McAfee Lab threat reviews and testing policy assignments against new threats. Administered email account requests from new users and maintained mail exchange structure. Monitored SIEM applications for any persistent threats to network. Performed security audits in according with NIST policies to reflect vulnerabilities and recommend changes. Performed monthly patching to workstations and servers as required by CYBER Security threats. Security Analyst member in directing security policies affecting new policies, reviewing identity and access management and file requests. Familiar with different security requirements for NIST, SOX, HIPPA, Splunk and SCADA requirements.

**Kipley A. Keene**

**EMPLOYMENT:**

**2015-8/2016-8 IS Security Analyst, Public Works Commission**

 Security Analyst.

 Security Compliance log audits.

 Issue VPN security requests.

 Configure Maintain, and Support Cisco ASA devices.

 Configure Maintain, and Support Cisco ISE for threats.

 Configure, Maintain, and Support Cisco IDS/IPS Sensors.

 Configure Maintain, and Support Antivirus software.

 Configure, Maintain, and Support email filtering software.

 Configure Maintain, and Support Web filtering software.

 Configure, Maintain, and Support user Security Certificates.

 Configure Maintain, and Support Cisco wireless network.

 Configure Maintain, and Support McAfee HBSS\EPO server.

 Configure Maintain, and Support McAfee Security Suites.

 Monitor network for Security, Performance, and User actions.

 Assist in client/server security, data access, IAM.

 Recommend and Implement new security protocols, procedures, and applications based on NIST compliance for SP 800-53

 Write Security/Compliance policies for organization.

**2010-2015 System Security Analyst, U.S. Army Operations**

 Network Administration

 Install and troubleshoot software and hardware issues for users.

 Troubleshoot system vulnerabilities.

 Administer SCCM and WSUS.

 Research configuration changes to software and hardware.

 Recommend and Implement new security protocols, procedures, and applications based on NIST compliance for SP 800-53.

 Administer McAfee EPO\HBSS, making machines compliant.

 Monitor system vulnerabilities using Fore Scout.

 Monitor domain with Nessus ACAS Tenable scanning software.

**2007-2010 Network Administrator, U.S. Army Special OPS**

 Network Administration

 Exchange Administration

 ESXi Administration

 NetApp Administration

 Active Directory Administration

 Install and troubleshoot network server and domain activity.

 Desktop support for Microsoft applications and share connectivity.

 Recommend and Implement new security protocols, procedures, and applications based on NIST compliance for SP 800-53.

 Build and repair servers.

**2001-2007 Network Administrator, U.S. NAVY**

* Retired Navy Cryptologic Maintenance Network technician
* Network Administration
* LAN Administration
* Training IT Administrator
* Exchange Administration
* Active Directory Administration
* Install and troubleshoot network server and domain activity.
* Desktop support for Microsoft applications and share connectivity.
* Recommend and Implement new security protocols, procedures, and applications
* Provide technical expertise in network-centric operations.
* Detect, protect, react and respond to threats against Navy networks.
* Defend against external and internal threats through in-depth technical and non-technical methods.
* Computer Network Risk Mitigation.
* Network Vulnerability Assessments and Incident Response/ Reconstruction.
* Active computer network defense, access tool development and computer/network forensics.
* Build and repair servers.
* Qualifications and Interests CTMs must learn advanced computer, network, and electronic system troubleshooting methods based on complicated technical concepts. They must be resourceful, logical and possess an average degree of manual dexterity and be of exceptional character. Applicants must be U.S. citizens and meet eligibility requirements for continuous access to sensitive compartmented information (SCI). Eligibility

for a top secret clearance is determined by the results of a Single Scope Background Investigation followed by a reinvestigation every five years. Normal color perception and normal hearing are required.

**TRAINING:**

 Security Analyst Administrator

 Tenable Administrator (Vulnerability Management)

 NIST, ISO, HIPAA (Vulnerability Management)

 System Administrator

 Fiber Optic DOD Instructor

 Help Desk Administrator

 McAfee EPO\HBSS Administrator

 Microsoft client and server builds

 CEH FED VUE Course

**CERTIFICATIONS:**

 Comptia Security+ Certified

 Adjunct Information Technology Instructor

 ATM Switch Certified

 Working toward CISSP Certification

**SOFTWARE COMPETENCIES:**

Microsoft Windows XP/7, Windows Server 2003/2008/2012, Microsoft Office

2003/2007/2010/2013, Open Office, Wireshark, Microsoft Visio 2003/2010/2013, McAfee ePO; McAfee Suite; Triton Websense; Barracuda Email Firewall; VIPRE

Antivirus; Symantec Antivirus; Lumension Security; Airwatch, Tenable vulnerability assessment

**AREAS OF EXPERTISE:**

Problem Solving; Troubleshooting;; Communications; Technical Research; Information Security; Antivirus; Device Encryption; Email Filtering; Web Filtering; TCP/IP; Policy/Procedure Development; Compliance; VLAN; LAN; WLAN; VPN;

Cisco ASA; Routing Protocols; Broadband; DSL; Mobile Device Management; Active Directory; Group Policy; Device Control; Patch Management; Software Implementation; McAfee Security Suite, Risk assessment.

**EDUCATION:**

2009-2011

 Kaplan University BS Degree in Information Technology

2004-2005

 University of West Florida Certificate Information Systems Technology

**AREAS OF EXPOSURE:**

McAfee DLP; McAfee HIPS; McAfee SIEM; Risk Management; Security Assessment; VM Environment; System Analysis; Management; Application Control; Testing; Network Performance; Cisco ISE; Load Balancing;

DNS, ACAS NESSUS, Tenable, Sourcefire, Splunk evaluation, NIST FIPS 200 and FIPS 199 compliance guidelines

**PROFESSIONAL MEMBERSHIPS**

Security email list