Sean C. Cooper

Summary

I am an experienced, versatile and reliable security professional with a focus on infrastructure/platform security, network security, and platform hardening. I am also a natural communicator and team leader.

Education

Technical	VMware ESX	ITIL / ITSM Service Framework	CompTIA Security+
	VMware vSphere/vCenter	CIS Critical Security Controls	DoD Information Assurance
	Active CISSP	PCI Standards PCI-DSS 3.1	RedHat Enterprise Linux
	Docker Container Security	Certified Solaris SysAdmin	Risk Decision Acceptance
	Rapid7 Nexpose CSA	Certified AWS SysOp	NIST 800-series

Awards, Adjudications & Honors

J. Crew Group, Inc.	• Yearly Performance Bonus, Every Year Eligible, 2017-2019
AppNexus	• Quarterly Performance Bonus, Every Quarter Eligible, 2014-2016
Department of Defense	• Inactive Federal DoD Security Clearance: Top Secret
Visual Data Systems	• Employee of the Year – December 2008, DIS Team Award – April 2008

Work Experience

J. Crew Group, Inc. — **Manager – Information Security, Deputy CISO** — April 2017 – Current

- Designed and implemented J. Crew's first cloud-computing (AWS) security framework for the eCom division.
- Conducted successful PCI DSS 3.2.1 audit of internal systems and controls for Level 1 Merchant and Provider.
- Composed and revised InfoSec policies to bring them in line with modern security standards and best practices.
- Designed, implemented, and documented the J. Crew vulnerability management program and technical systems.
- Performed RFP technical evaluations for enterprise projects to judge suitability for implementation.
- Managed and coached information security analysts, including tasking, strategy, and performance evaluation.
- Introduced the "fail-forward strategy" to information security team, assuring progress even if POC/goal failed.
- Proposed, constructed, and delivered information security curriculum for staff professional development.
- Mentored subordinates and teammates as needed on industry best practices, standard operating procedures, etc.
- Designed, proposed, and implemented in-house standards-compliant incident response and forensics capability.
- Recruited VIPs to facilitate the security mission and narrative: "enabling users to do their tasking in a secure way."
- Modernized the information security team's collaboration and ticketing/service desk capability.

AppNexus — **Senior Information Security Analyst** — Oct 2014 – December 2016

- Improved holistic security posture through implementation of technical and policy controls of information systems.
- Achieved 40% reduction in plant-wide vulnerability score of ~25,000 production information systems in 1.5 years.
- Sat on the AppNexus CyberSecurity Steering Committee as a founding member.
- Executed and oversaw external penetration test against our systems as lead technical resource.
- Mentored and coached junior members of the CyberSecurity team to increase performance, work product quality.
- Prepared project architectural designs, technical and operational documentation, costing summaries, SOPs, etc.
- Designed, implemented, documented and sustained a vulnerability management process and scanner (Nexpose).
- Drafted, reviewed, revised information security policy documents and web/wiki pages.
- Designed, implemented a customized cross-functional investigation workflow for bad-actor email inboxes.
- Lead frequent multi-person, cross-team efforts to migrate or update system to address vulnerabilities.
- Authored a whitepaper outlining security best-practices and baselines to secure a rapidly growing Docker infrastructure.
- Analyzed CentOS, Ubuntu, OS X, network gear, appliances, and other equipment for best-practice configurations.
- Provided incident response subject matter expertise and elbow-grease to Service Desk, System Operators, as needed.

Brooklyn, NY, USA resume@seancooper.nyc (302) 492-7326

Sean C. Cooper

Solomon Page Tech — **Information Security Consultant** — Sept 2014 – Oct 2014

- Utilized subject matter expertise to provide consulting services directly to client on IA/IT subject matter.
- Performed security assessment to identify security flaws in workstations, servers, networking gear and policies.
- Provided action plan to secure and remediate flaws in workstations, servers, network and policies.
- Performed external security scans to identify unusual service availability, network configurations.
- Performed internal security scans using Nessus, Wireshark to identify software vulnerabilities in workstations & servers.
- Evaluated customer-provided security and policy documentation for completeness, compliance with best-practices.
- Created and maintained policy documents to client to supplement missing/inadequate IT/IA policies.
- Cultivated and maintained great customer relationship through dedication and high-quality output products.

DISA — **Principal CDES Architect** — Sept 2010 – Aug 2014

- Provided technical guidance and leadership in the evaluation, selection, testing and implementation of guard solution.
- Delivered policy and technical guidance in relation to customer engagements and internal technology development.
- Delivered and implemented standard operating procedures, architectural diagrams and engineering artifacts for consumption by internal and external customers.
- Provided full-scope technical support of all layers of operations, including Cisco networking, Windows platforms, *nix platforms, custom-built operating systems.
- Acquired, installed, configured, operated and maintained an enterprise-grade VMware ESX 5.x virtual infrastructure, including VMware ESX 5.x Hypervisor, VMware vSphere, shared storage, virtual switching, trunk port aggregation.
- Performed functionality and security analysis of systems for detection/prevention of threats.
- Achieved CISSP (Certified Information System Security Professional) certification through ISC2.
- Sat on DISA Cross-Domain Request Evaluation Committee, delivering decisions about feasibility of CDES requests.

JIEDDO — **Senior Systems Engineer** — March 2010 – Sept 2010

- Supported the DoD in its mission to provide rapidly evaluated and funded technology grants to researchers.
- Provided remote and in-person support for highly available, classified, networked RedHat Linux ES production system.
- Configured BIND, Sendmail, Postfix, vsFTPd, Samba, PPTP VPN server, Apache, MySQL to offer services to clients.
- Installed, configured and maintained approximately 40 RedHat Enterprise Linux 4 servers in a production environment.
- Allocated, provisioned and configured StorageTek network storage using Common Array Manager.
- Remediated vulnerabilities using the DoD IAVM system by installing patches and changing configuration parameters to utilize DoD STIGs.
- Created, modified and maintained `bash` scripts for system tasks such as backups, synchronization of files, user manipulations, and other miscellaneous tasks.
- Installed, configured and maintained VMware ESX 3.x and VMware ESXi 4 servers using high-availability principles.
- Configured and maintained networking equipment such as BigIP F5, Cisco switches, Linux-based NAT router.
- Delivered comprehensive documentation for systems inherited from previous employees and subcontractors.

NSF — **Tier 3 Helpdesk Lead** — July 2007 – March 2010

- Provided leadership for the National Science Foundation's Infrastructure as Team Lead of the Tier-3 Ticketing Team.
- Served as a liaison for different infrastructure teams to the Tier 3 Help Desk team.
- Mentored junior help desk technicians and engineers in skills acquisitions, standard operating procedures, etc.
- Active Directory manipulations of user accounts, email attributes, mailboxes, profiles and information.
- Documents and processes provisioning, modification and termination of user accounts.
- Engineering review and system administration of VMware ESX 3.x infrastructure and upgrades.
- Expert troubleshooting and diagnostic of Windows, Mac and Linux systems.
- Cisco networking device configuration of speed/duplex, NAC, port security and port diagnostics and configurations.
- Gathering forensic evidence for OIG staff used in decision-making and prosecution for civil and criminal activity.
- Prepared detailed, plain-language technical analysis and consultation to non-technical OIG staff.

Brooklyn, NY, USA resume@seancooper.nyc (302) 492-7326