**Eric M Foos**

**Network Security Engineer**

**804-366-4311**

**Eric.foos@ecstech.com**

|  |  |  |
| --- | --- | --- |
| Education | | |
| B.S. in Urban Studies and Geographic Information Systems, Virginia Commonwealth University | | |
| Relevant Training and Certifications | | |
| **TECHNICAL SKILLS & CERTIFICATIONS:**  **Operating systems:** Server 2012 R2, Server 2008 R2, Server 2003, Windows 10, Windows 7, XP, Cisco IOS, RHEL 6 & 7, Kali Linux, SIFT, Ubuntu Server.  **Virtualization/Cloud:** VMware vSphere 6, AWS, Microsoft Azure, OCI  **Log aggregation/correlation:** Splunk, ELK stack  **Languages:** Python  **IT Certifications:** GCIH, Security+ | | |
| Clearance Level | | |
| Top Secret | | |
| Professional Experience Highlights | | |
| * Extensive experience engineering and administering Information Security tools to maintain the confidentiality, integrity, and availability of customer information technology systems. * Significant experience performing intrusion detection, incident handling & response, digital forensics, and malware analysis. * Adept at vulnerability and threat assessment from executive level reporting to individual system remediation. * Demonstrated success configuring and managing Server, Network, and Storage infrastructure to support business security and operational objectives. * Knowledgeable in VMware vSphere virtualization platform, various Windows Server roles, and Linux distributions. | | |
| Chronological Experience | | |
| ECS Federal, LLC; Network Security Engineer | | 04/2019-Present |
| * Designs, builds, and tests network security solutions for customer enterprise environments to protect confidentiality and integrity of customer data and provide consistent availability of customer information technology systems. * Performs design, testing, and implementation of application layer security solutions including cloud-based internet isolation. * Designs and configures AWS Govcloud Virtual Data Center Security Stack (VDSS) architecture using the Transit VPC design to enable secure transport of customer data to and from the cloud. * Performs testing and implementation of AWS compute and networking components including EC2, VPC, IGW, VGW, AWS Direct Connect, Security Groups, NLB/ALB/ELB, etc to assist in customer workload migration efforts. * Performs testing and configuration of AWS Identity and Access Management as well as AWS Organizations to consolidate account management and security through the principles of least privilege and controlling blast radius. * Tests and utilizes various Infrastructure as Code solutions including CloudFormation, Lambda, Terraform, and Ansible to automate the provisioning of new resources and configuration/security of existing resources. * Performs testing and configuration of virtual networking and security solutions including Cisco Cloud Services Router, Palo Alto NGFW, and F5 ASM (WAF/SSLO). * Builds and maintains detailed documentation of network and security solutions implemented to assist operations and sustainment teams maintaining said solutions. * Designs and tests VDSS transit VNET/VCN architecture in Microsoft Azure and Oracle Cloud to meet customer requirements to migrate to various Cloud Service Providers (CSP). | | |
| ECS Federal, LLC; Network Security Monitoring Watch Officer/Analyst | | 04/2017-04/2019 |
| * Performs analysis of indicators of compromise against customer assets and performs efficient triage of potential intrusions. * Makes extensive use of Splunk Search app to query customer data set for both threat hunting and effective incident response. * Evaluates and tunes indicator of compromise logic to perform threat hunting of known APT tactics, techniques, and procedures.. * Coordinates incident handling efforts to identify, contain, and eradicate threats against corporate or customer assets. * Performs host vulnerability analysis using Tenable SecurityCenter and Nessus to effectively correlate vulnerabilities to potential intrusions. * Performs file system and memory captures using Encase to gather evidence and artifacts on compromised hosts. * Utilizes Volatility to perform in depth memory analysis in efforts to detect evasive malware. * Uses SIFT workstation and custom reverse engineering toolsets to perform static and dynamic analysis of malware. * Analyzes IDS alerts that fire as a result of Suricata and Fidelis signatures. | | |
| OMNIPLEX World Services Corporation; Security Engineer | | 09/2016-04/2017 |
| * Installs, configures, and manages Information Security tools and supporting systems/network infrastructure to address enterprise security gaps and initiatives. * Conducts network and system vulnerability assessments using Tenable SecurityCenter and Nessus. * Coordinates monitoring and incident response efforts to identify, contain, and eradicate threats against corporate or customer assets. * Utilizes behavior based detection products and methodologies to perform threat hunting of APTs. * Performs Memory forensics using Redline and Rekall to analyze and detect evasive malware. * Uses REMnux reverse engineering distribution for static and dynamic malware analysis. * Implements, monitors, and audits Cisco ASA 5585 firewall rules and Cisco Firepower IPS policies. * Configures and monitors several behavior based detection products such as Rapid 7, Varonis, and FireEye ETP. * Responsible for enterprise vulnerability remediation efforts including Patch Management and STIG OS hardening for 500+ node environment. * Responsible for regularly briefing executive management on cyber threats, escalated incidents, and new technology to improve security posture. * Administers TrendMicro OfficeScan for agent based endpoint AV solution and TM Deep Security for agentless virtual server protection. * Manages Symantec DLP solution to identify exposed PII on file servers and address access control deficiencies on corvporate file shares. * Performs configuration, management, and troubleshooting of enterprise VMware vSphere 6 environment consisting of multiple vCenter servers and ESXI HA clusters utilizing DRS and vMotion. * Experienced with NetAPP SAN Configuration and Management, NAS and SAS, LUN & Mapping, and RAID groups. * Performs Windows Server administration including Active Directory, Exchange, DNS, DHCP, IIS, File Server to maintain high availability of production environment. * Configures Cisco UCS FlexPod blade servers, Catalyst and Nexus switches, and ASA Firewall/VPN | | |
| BAE Systems, Inc.; SOC O&M Lead/Cyber Security Analyst | | 05/2015-09/2016 |
| * Leads efforts for SOC O&M team to provide consistent availability and accuracy of all SOC Security tools. * Responds to and conducts analysis of possible security events or incidents that occur against customer enterprise network. * Configures and maintains Tenable SecurityCenter for enterprise wide system vulnerability assessment and reporting. * Utilizes McAfee ESM for event log aggregation and correlation to perform threat analysis. * Participates in the design, planning, configuration, and operation of SOC Security tools. * Performs configuration and administration of SOC VM infrastructure using vSphere Web client, vCenter, and ESXi hosts. * Manages HP WebInspect tool and conducts vulnerability assessments of customer Web Applications. * Administers Trustwave AppDetective Pro database scanning software for vulnerability assessments of Oracle and SQL Server databases. * Performs extensive support and training to customer ISSO and SA community on vulnerability assessment and change management processes. * Provides configuration, troubleshooting, and maintenance for Cisco ASA 5505 VPN concentrators that are used at remote customer sites. | | |
| Attotek, Inc.; Systems Engineer | | 03/2012-05/2015 |
| * Configured and maintained server and data storage infrastructure in both production and test development environments * Designed and configured hardened operating system images to be deployed in TS/SCI environments. * Routinely scanned, conducted vulnerability assessment, and performed remediation for roughly 50 production and test development servers. * Operated VMware to create a number of server templates utilizing various hardware and software configurations to efficiently deploy new systems, provide fault tolerance, test new software builds and patches, and reduce footprint. * Configured and administered Cisco ASA firewall to support local and remote user base. * Regularly worked with senior development staff to debug java based application software. * Used Camtasia Studio to develop demonstration videos of software best practices and features. | | |
| Wells Fargo Advisors; LAN Analyst | | 09/2011-03/2012 |
| * Provided WFA domain administration through Active Directory. * Evaluated third party software installation requests from end users to determine whether said software could compromise information security. * Created custom OS images to fit each end user group’s specific needs. * Provided technical support to field technicians installing or repairing hardware. * Configured Windows XP VMs to run customer apps not compatible with newer operating systems. | | |
| **Attotek; Junior Systems Administrator** | **05/2009-08/2010** | |
| * Performed administration of Windows Server 2003 servers to support business efforts. * Performed health and monitoring for all storage hardware. * Assisted in maintaining availability and uptime of business preprocessing data efforts. * Created graphical representations of digital terrain elevation data. * Provided desktop support for company employees to include troubleshooting hardware and software issues. | | |
| **Blanton, Kirk, and Lumpkins, PLC; Data Management Assistant** | **12/2008-05/2009** | |
| * Assisted in company migration to the latest version of ProLaw software suite. * Updated legal database records to remove outdated entries and standardize formatting. * Assisted company employees with technical support for Microsoft Office and Prolaw related issues. * Troubleshot hardware issues for on site employees. | | |