SARAHHAMPTON

Security Data Engineer

Experience

Senior Security Operations Engineer, HomeAway — *May 2015 - Current*

Built HomeAway's Security Operations Center from the ground up, including: managing Splunk Enterprise Security search heads/indexers, importing/parsing data into Splunk environment, automation of security actions, metrics around security operations, building advanced threat models, incident response procedures, management for HomeAway's 24/7 SOC in Lima, Peru.

-> Building security policy, detection, and automation in the AWS environment.

-> Creating python scripts utilizing the APIs of security tools in order to automate *all* actionable incident response tasks. These include containing a device off the network, automatically blocking on URL or IP, auto-generating Jira ticket based on a security incident or the results of a vulnerability scan, and API pulls of online security tools (i.e. VirusTotal) to have additional intelligence.

Security Network Engineer, Phillips 66 — *May 2013 - April 2015*

Administrated and maintained Phillips 66's Security Environment (firewall/proxy/nac), including firewall rule implementation/troubleshooting, firewall migrations, security reviews, PCI compliance, VPNs, IDS/IPS, NAC, scripting the automation of network security processes.

-> Built a logging standard and strategy using a Splunk environment for Phillips 66 integrating routers, switches, wireless devices, firewalls, proxies, SIEM, DLP, ServiceNow, and built custom scripts via APIs.

-> Implemented Cisco ISE for NAC (Network Access Control) in remote shared offices. Working with the business users to create security policies for posturing and profiling of devices.

-> Acted as Solutions Integrator for the redesign of Phillips 66's Blue Coat proxy environment. This was a redesign from a explicit to a transparent proxy deployment that included inspecting SSL, custom URL categorization.

Web Infrastructure Analyst, ConocoPhillips/Phillips 66 — *February 2011 - June 2013*

Installed, configured, and participated in troubleshooting applications on IIS, Websphere, and Apache for application support on Windows 2003/2008 server environments.

-> Saved hundred of hours on the hardening process by developing a powershell script that changes/verifies IIS settings, registry keys, and permission standards for Windows 2008 R2 servers that could be executed on multiple servers in a single process.

-> Created and executed an automated compliance process for server 2008 R2 using Powershell and Microsoft SQL server to identify insecure processes and ensure success in upcoming audits.

-> Built Phillips 66's internet, extranet, and intranet environments during the divestiture of Phillips 66. This included hardening over 600 servers, Siteminder and Netscaler configuration, internal DNS, AD group creation, software installation, and working with application support for Microsoft 2003 and 2008 servers.

Common Operating Environment Analyst, ConocoPhillips — *June 2010 - February 2011*

Acted as part of a Proof of Concept project for implementing a managed desktop company-wide desktop environment and an upgrade from XP to Windows 7. Evaluated endpoint products that could be eliminated, replaced, or added to the standard PC image.

Database Administrator, Reality Check, Inc - Non-Profit — *June 2008 - May 2010*

While a full-time student at the University of Arkansas, developed a participant tracking system for a non-profit. Saved hundreds of hours of manual data collection and was successful enough to share with other non-profits struggling with the same situation.

Education

University of Arkansas, Sam M. Walton College of Business, Fayetteville

Bachelors of Science in Business Administration, Information Systems, May 2010

Security

SIEM:

Splunk ES
QRadar
Netwitness

Network:

PaloAlto FW/IPS
Cisco ASA FW/IPS
CheckPoint FW
BlueCoat Proxy
Cisco ISE (NAC)
Protectwise
ClearPass (NAC)
Incapsula WAF
Imperva WAF
SecureTrack
Netscaler

Endpoint:

Symantec AV
FireEye HX
Symantec DLP
BigFix

Technologies

Windows Server
Linux Server
SQL Server
Active Directory
DNS
AWS

Languages

Python
Powershell
SQL
SPL
Visual Basic
Bash
Expect
Perl

11119 Alterra Pkwy, Apt 1226
Austin, TX, 78758

sarah@hampton.wtf

512-234-2526