PAUL FORST

Information Security Engineer

Massapequa Park, New York

1-516-620-2375

Paul@forst.io

cv.forst.io

PGP: bit.ly/pgp-forstio

Skills

Security Awareness

Delivering security awareness training to associates.

Documentation

Documentation of Information Security Operational Systems.

Policy Creation

Creation of Information Security Policies

Vulnerability and Risk Management Software

Nexpose, Kali Linux, Metasploit

Multifactor

Experience with the following: Duo Security, RSA SecurID, Symantec VIP

SIEM

Expierence with the following: QRadar, Nitro/Mcafee, LogRhyhtm, Splunk

Endpoint Protection

Summary

Detail-oriented, highly skilled Information Security Engineer with over 15 years of expertise in information technology including risk management, system hardening, and malware prevention, detection and removal. Innovative problem solver whose strong critical thinking skills yield forth inventive and effective approaches to the organization. Consistently achieving and surpassing objectives through creative dynamic contributions of organization, communication and leadership capabilities. Able to flourish in a fast-paced, exciting environment where precision and productivity matter.

Work experience

April 2015 - Present

Information Security Engineer

The Natures Bounty Co. (Formally NBTY)

Engineer and Implement security solutions to enhance the data protections of the organization following best practices.

- Implemented DUO multifactor
- Implemented Corporate password reset tool
- Policy engineered and facilitated the implementation of Cisco Identity Services Engine
- Implemented Microsoft LAPS
- Implemented Cisco Umbrella formally OpenDNS (Replacing Cisco Ironport Proxy)
- Designed firewall changes workflow for approvals and change execution
- Manage Symantec Endpoint Protection 14 policies and oversee the operations
- Implemented security.txt for use on our ecom site
- Implemented Ironkey encrypted USB storage
- Developed endpoint firewall policies for our UK retail environment
- Implemented a global DDOS protection solution
- Implemented and maintain an employee monitoring system
- Designed safeguards around wire fraud phishing emails
- Assist the information security analysts with investigations
- Create basic dashboards and alerts within Splunk
- Maintain Stealth Intercept (AD & File) monitoring system
- Participate in annual policy reviews
- Review security bulletins, assess impact, and work with teams to implement updates
- Review new security products and make recommendations on purchases
- Provide articles for our internal IT newsletter

May 2012 - April 2015

Information Security Analyst

NBTY

Transitioned from the Data Center Operations Group to Information Security Group. Responsible with overseeing NBTY's Vulnerability Management Program. This includes assessing the security of systems deployed including, external web servers, internal servers, workstations, and point of sale systems.

• Evaluate system security using advanced tools such as Nexpose and Metasploit to identify and confirm system vulnerabilities, assess the severity of these issues and resolve weaknesses with responsible stakeholders with remediation plans

• Manage SIEM Solution and track incidents in our internal ticketing system

• Executed whole disk encryption to protect notebooks

• Collaborate and maintain ongoing security policies and controls to strengthen NBTY's security posture

Symantec Endpoint Protection

Firewalls

Management of Checkpoint, and Sophos UTM Firewalls.

VMware

VMware ESX/vSphere 5.5 and 6.0

Proxy Servers

Manage Proxy Server Policies for Ironport, and Bluecoat proxy servers.

Training

SANS	GIAC: Security Essentials
VMware:	
	vSphere 5 [Install, Configure, Manage]
	NSX 6: [Install, Configure, Manage]
Splunk	Splunk 7.0 Fundamentals Part 1
	Splunk 7.0 Fundamentals Part 2
	Splunk Enterprise Security 4.7

Certifications

ITIL V3

Security+ (2015-2017)

SSFIPS (Cisco SourceFire)

• Control endpoint security utilizing Symantec Endpoint Protection in a global environment

• Responsible for Internet proxy configurations, policies and reports

• Document the architecture of information security systems

• Create documentation to assist associates with the enrollment of security services

• PCI Compliance V3.0

Feb 2010 - May 2012

Data Center Operations

NBTY

Responsible for deploying, maintaining and troubleshooting servers in the data center along with remote branches and subsidiaries. Managed over 1500 physical and virtual servers.

- Deployed virtualization technologies remotely to reduce expenditures of multiple servers
- Participated in monthly patching of critical infrastructure systems
- Assisted help desk staff to expedite advanced troubleshooting of complex issues and resolved issues without need for further escalations
- Supported and cultivated both physical and virtual servers with hardware and software upgrades
- Monitored the computer environment utilizing tools such as HP insight Manager, Solarwinds Network Performance Monitor, IPSwitch, What's Up, Solarwinds Virtualization Manager, and Microsoft System Center Operations Manager to get a detailed view into the health of the environment
- Utilized tools such as Twitter and corporate blog sites, to assess security vulnerabilities that may impact patching cycles
- Tracked and regulate trends in current security attacks
- Executed daily checks of the data center to scrutinize for any issues or concerns before problems arise

Jul 2007 - Feb 2010

Systems & Networking Administrator

AON (Acquisition of Allied North America)

- Manage all aspects of users and security using Active Directory and Microsoft Exchange.
- Manage and document group policy changes
- Troubleshoot, Patch, Upgrade, Cisco Call Manager and Cisco Unity Messaging.
- Add new devices in Cisco Call Manager, and create/change/delete voicemail accounts in Cisco Unity Messaging.
- Evaluate and recommend new software to be implemented throughout the organization.
- Maintain and Install Riverbed WAN Accelerators for branch offices.
- Maintain Cisco Maintenance Contracts.
- Assist service desk with issues that pertain to the systems side of the business.
- Implement, Deploy and Maintain VMWare vSphere 4.
- Maintain and support Equal Logic iSCSI SAN adding new storage and replica volumes.
- Maintain and support BlueCoat Proxy server.
- Responsible for maintaining and supporting our Citrix Xenapp farm.

Feb 2004 - Jul 2007

Systems & Networking Administrator

Natural Organics Inc.

- Configured and deployed new data connections for the new warehouse location in Reno, Nevada, including frame relay, T-1 internet services, BDCs, fiber optic network, desktops, network printers, VOIP phones, tape backup, battery backup systems
- • Troubleshoot, and maintained 3 Citrix servers, Exchange 5.5, Checkpoint 4.x firewall, Cisco 3600, 2900, 2800, 1621, and 831 routers. Nortel Baystack 350 switches with Power Over Ethernet(POE),NT 4.0 domains, Active Directory, BrightMail anti-spam solution
- Upgraded existing routers to newer IOS, and changed service providers

from AT&T to Sprint, replacing frame relay and internet connections for New York headquarters
- Migrated from Exchange 5.5 to Exchange 2003 along with a migration to AD
- Maintained and upgraded Apple G4 workstations running OS9 to Apple G5 workstations running OS X and upgraded to gigabit switching
- Setup network monitoring software to monitor and alert critical bandwidth issues occurring in real-time
- Reviewed/Modified Internet monitoring software. Update tables and restricted sites; created restricted group levels for warehouse employees to prevent internet abuse
- Maintained 100+ printers within the organization
- Changed/Modified top level domain servers for 150+ domain names
- Assisted SAP basis administrators and ABAP programmers with system specific needs as they occurred
- Created Visio flowchart diagrams to document network infrastructure for management to understand and follow system upgrade needs, while explaining in non-technical terms why upgrades for software and hardware are necessary
- Setup fax server for customer service department to expedite faxing to customers, saving time and money by efficiently queuing fax messages through Microsoft Exchange server with GFI fax server
- Maintain, and monitor nightly tape backup jobs utilizing Symantec Backup Exec.
- Configure VOIP phone and Cisco 831 router for IPSEC tunnel to Reno for a SOHO data link

Dec 2001 - Feb 2004

Partner

Next Age Technologies

Installed CCTV systems on weekends for 30+ customers and maintained, upgraded, repaired systems.

Sep 1999 - Feb 2003

Jr. Network Administrator

TechSmart.com

- Installed and maintained computer systems and internet connections for corporate offices and remote office locations across the U.S
- Responsible for the maintenance of multiple mission critical servers, as well as user workstations
- Maintain tape backup library, which includes backing up of corporate exchange servers, file servers, and SQL databases
- Responsible for auditing, tracking, accounting, and supporting over 30 laptops for staff and executives throughout the United States
- Installation, upgrading, maintaining, troubleshooting, and tracking, of all office equipment in corporate offices
- Troubleshoot network and PBX problems throughout the corporate offices
- Update management during weekly status meeting in regards to current projects and procedures, new developments, and the status of special projects
- Develop and implement training and cross training procedures for staff and executives
- Assist employees with all computing needs

Education

Sep 1995 - Sep 1996

Computer Information Systems

Suffolk Community College

- Jun 1995

Connetquot High School