Chad Porter

CYBER SECURITY PROFESSIONAL

1260 SE Waddell Way, Waukee, IA 50263

(515) 865-0880 | chadaporter@gmail.com | www.chadporter.net | chadporter | chadporterdev

Technical Skills

Penetration Testing Tools - Rapid7 Nexpose, Nessus, PhishingBox, Metasploit, Burp Suite, OWASP Zap, Nmap, OpenVAS, Nessus, Wireshark

Network Administration - Cisco ASA, MikroTik, SonicWALL NSA, Fortinet Fortigate, BIND DNS management, VPN administration

System Administration - Hyper-V, ESXi, UNIX/Linux Server, Windows Server 2019-2008, Active Directory, Group Policy, WSUS and SCCM, Puppet, Docker, Ansible, SQL Server database design and implementation

Languages/Methodologies - C#, ASP/MVC/VB.NET, Python, PowerShell, jQuery, Perl, PHP, Ruby, and Go

IDEs / Frameworks - Visual Studio 2019-2013, .NET Framework 4.8-3.5

Software Platforms - Windows 10, Windows 7, and Legacy OS Administration, FortiSIEM, QRadar

Certifications

WIP	**OSCP**	- Offensive Security Certified Professional
2018	**GCIA**	- Certified Intrusion Analyst (GIAC)
2016	**CSSP**	- Certified Security Professional (SonicWALL)
2015	**CSSA**	- Certified Security Associate (SonicWALL

Work Experience

Pratum   *Ankeny, IA*
SOC ANALYST II   *Sep. 2019 - Present*

- Perform event correlation on security incidents from sourced metadata on Fortinet SIEM appliances
- Research, analysis, correlation, and reconstruction of attacks from a wide variety of data sets
- Identify and analyze anomalies in network traffic using metadata
- Develop and implement custom attack signatures on cyber defense network tools in response to analyzed threats
- Validate intrusion detection system (IDS) alerts against network traffic

Pratum   *Ankeny, IA*
INFORMATION SECURITY ANALYST I   *Sep. 2017 - Sep. 2019*

- Analyzed and responded to security incidents from Fortinet SIEM appliances
- Analyzed requirements for various projects, risk analysis, and installation, configuration and maintenance of both physical and virtualized SIEM appliances
- Developed threat mitigation strategies, policies, and incident response procedures consistent with business strategies while effectively protecting data integrity, security, and limiting liability
- Increased efficiency of alerts and reports through scripting automation
- Performed vulnerability analysis and implemented corrective and preventative actions
- Maintained SIEM engine rules and created trend-based rules to reduce IT systems risk
- Developed and executed remediation strategies to maintain high availability

OXEN Technology   *Ames, IA*
TECHNICAL ENGINEER   *Dec. 2015 - Sep. 2017*

- Managed and administered daily operations of 40+ servers running Windows Server 2016-2008
- Analyzed requirements for various projects, risk analysis, and installation, configuration and maintenance of both physical and virtualized servers through Hyper-V
- Developed IT strategies, policies and incident management procedures consistent with business strategies while effectively protecting data integrity, security and limiting liability
- Reduced infrastructure costs by moving physical servers running Windows Server 2008 to Microsoft Azure
- Managed 80+ SonicWALL/Sophos firewalls, including preparation for security audits
- Performed vulnerability analysis and implemented corrective and preventative actions
- Maintained host based firewall policies and reflected those policies on network firewalls
- Developed and executed scripts for automating tasks on servers under my responsibility

ICS Advanced Technologies

NETWORK OPERATIONS TECH / CUSTOMER SERVICE

Ames, IA

Dec. 2012 - Sep. 2015

- Managed 200+ Cisco routers, switches, and access points providing stability and high availability for a complex network
- Deployed intrusion detection system increasing performance with internet traffic control
- Cooperated with network engineering teams in project management from initial customer needs assessment through product development, deployment, user training, and documentation
- Linux-based Layer-3 router and switch management with agile update deployments
- Linux-based Layer-2 switch fine-tuning, performance improving and standardizing configurations and scripts based on ITIL methodologies

Bratney Companies

IT SOLUTIONS DEVELOPER

Des Moines, IA

Apr. 2012 - Aug. 2012

- Designed and developed web, console, and Windows applications in a .NET 4.5 environment
- Cooperated with system administrators in desktop support and server management
- Microsoft SQL Server administration – backups, data migration, and data replication
- Involved in planning of multiple complex business projects focusing on cost-effectiveness

Wells Fargo

DATA ENTRY / CLERICAL

Des Moines, IA

Apr. 2009 - Jul. 2009

- Performed basic data entry of loans
- Assisted field employees with loan applications
- Team workflow improvement strategies

Education

Iowa State University

MAJOR - MANAGEMENT INFORMATION SYSTEMS

Ames, IA

2011 - 2014

Des Moines Area Community College

INFORMATION TECHNOLOGY/NETWORK ADMINISTRATION, ITNA

Boone, IA

2009 - 2011

- Computer hardware maintenance
- Windows networking and domain management
- Cisco CCNA training

Projects

WinRM-Shell Source: https://gitlab.com/chadporter/winrm-shell

Activities / Interests

- Penetration testing, intrusion detection, firewalls, and vulnerability assessments
- Cryptography, data forensics, and disaster recovery
- Freelance graphic design
- Freelance web design / development