Danny Weng

Security Analyst

(617) 230-7506 | me@dannyweng.com | dannyweng.com | dannyweng | dannyweng

Skills

Programming	SPL, Python, Bash, PowerShell, SQL, JavaScript, HTML, CSS, LaTex
Security Tools	Varonis DatAvantage, Sophos AV/SafeGuard, SentinelOne, Office 365 DLP, Dell SecureWorks, LogLogic SIEM, ZScaler, EnSilo, ProofPoint PPS/TAP/TRAP, CyberARK, Rapid7 InsightVM, Security Scorecard, HackerOne, Crowdstrike, Splunk
Vulnerability Scan	NMap, OpenVAS, Nessus, Wireshark, Aircrack, Shodan, Nikto
Penetration Testing	Metasploit, Burp, Armitage, OWASP-ZAP, Wireless cracking, and manual packet inspection
Virtualization	VMware vSphere, VirtualBox, Hyper-V, Citrix
Operating Systems	Windows Server, Parrot Security OS, Kali, Ubuntu, SUSE
AWS	EC2, S3, VPC, IAM, Route53, ELB, Cloudfront, RDS, Lambda, CodeCommit, CodeDeploy, Cloudwatch
Others	Office 365, Active Directory, Splunk, Salesforce, JIRA, Confluence, ServiceNow, Nagios

Certifications

GIAC Security Operations Certified (GSOC)
CompTIA Security+ ID: COMP001021085931
ITIL v3 Foundation License ID: 02344221-01-QJUY
EMCIE (EMC Implementation Engineer, VPLEX Specialist)
EMCSA (EMC Storage Administrator, VPLEX Specialist)
Learning Tree Certified Specialist in Linux Administration
Fundamental Linux Administration Certification by Linux Academy

Experience

TJX Companies — *Framingham, MA*

Cybersecurity Threat Analyst II — *Nov 2021 - Current*

- Triage and respond to alerts to reduce the likelihood of security impact to corporate assets
- Respond to escalations from our managed security services provider
- Maintain and adhere to defined runbooks for daily tasks, suggesting process and documentation improvements
- Recommend preventative technology measures to reduce security risks
- Assist with incident response procedures, participating in playbook development and tabletop scenario exercises
- Suggest new monitoring and alerting use cases to expand visibility and coverage of the attack surface
- Assist with security and enterprise wide projects
- Maintain awareness of emerging threats, vulnerabilities, and attacks

Stanley Black and Decker — *Waltham, MA*

Cyber Security Analyst — *May 2019 - Sept 2021*

- Identify and analyze information security threats and events, and respond effectively to security incidents
- Investigate anomalous traffic to identify threats or indicators of compromise
- Work with Legal or Human Resources to perform investigations, as authorized and appropriate
- Works on information security problems that are diverse and highly complex
- Selects methods and techniques for identifying and advocating effective security solutions
- Develops approaches to address critical information security issues
- Leads HackerOne disclosure program and remediates disclosures across various teams

Invaluable — *Boston, MA*

Deskside Administrator — *May 2018 - May 2019*

- Support and maintain end-user computing worldwide in the organization by providing troubleshooting and resolution of hardware, software, and network issues. Create, maintain, document and implement standards for client-side hardware, software, and operating systems
- Record and document incident requests per standard Service Desk procedure
- Managed and responsible for all onboarding, offboarding, and account related issues of employees via Active Directory and Office365
- Assist Network and Application teams with complex technical tasks including debugging and supporting client computing systems
- Diagnose and repair client computing devices and peripherals in the field including but not limited to PCs, printers, PC-based computer software, smartphone devices and other end-user equipment or software as required
- Managed the migration of a new Endpoint Solution project for corporate environments
- Respond to the Data Subject Access Requests (DSAR) under GDPR Compliance standards

Alegeus Technologies

Waltham, MA

Information Security Analyst

May 2017 - Aug 2017

- Served as a liaison between the IT department and Information Security team on information security related topics
- Deploy, monitor, and manage Sophos Endpoint solution on client machines to meet security compliance
- Reduced numerous amount of unmanaged machines from Active Directory to reduce company's risk
- Researched and deployed Bitlocker total disk encryption Bitlocker to protect corporate sensitive information
- Maintained Kantech (Badges, Cameras) physical security system to ensure we meet requirement for compliance
- Managed security projects such as the deployment of Imperva WAF, Dell SecureWorks IDS/IPS and Office 365 DLP
- Managed and maintained Varonis DatAvantage, a file system monitoring system
- Research the latest IT security trends, provide senior IT staff with recommendations, enhancements
- Assisted ISO with security compliance and audit (PCI, HIPAA, SOC 1, SOC 2)

Dell EMC

Hopkinton, MA

Senior Analyst

July 2014 - May 2017

- Troubleshoot and provide solutions to customer's issues through Salesforce ticketing support system
- Investigate highly complex systems and networking environments relating to VPLEX and SAN
- Collaborates with VNX, VMAX, RecoverPoint, Cisco, Brocade and various host teams to provide complete solutions support
- Interface with many Dell EMC functional departments such as Engineering, Sales and Customer Service for escalated issues
- Linux administrative work such as resetting passwords, troubleshooting networking and analysis live firmware logs

Harvard Business School

Boston, MA

Technical Support Analyst (Contractor)

Jan 2014 - July 2014

- Installation, upgrade, configure, and deployment of Windows 7 and Mac OS
- Provided technical troubleshooting for staff, faculty and doctoral students
- Tracked and managed tickets via ServiceNow – Service Management
- Managed active directory, printer management and file share
- Troubleshoot WLAN and LAN issues
- Purge and restore backed up data on Malware infected machines

Education

Harvard University

Cambridge, MA

Master of Liberal Arts, Extension Studies, Information Management Systems

Completed 2020

Harvard Extension School

Cambridge, MA

Cybersecurity Certificate

Completed 2018

University of Massachusetts

Amherst, MA

Bachelor of Science in Information Systems

Completed 2013

Projects

linkAnalyzer

- Source: `https://github.com/dannyweng/linkAnalyzer`
- Tool that utilizes VirusTotal and other security DB to scan URLs for malware

HeyNurse

- Source: `https://github.com/dannyweng/HeyNurse`
- Project created on the Google Voice AIY platform with the capability to parse Google Fit data with voice commands

Professional Associations

FBI InfraGard, Boston Chapter Member

Military

Army National Guard

Massachusetts

Private First Class

Oct. 2011 - Nov. 2012

- Secret Clearance - Inactive