ODAIL STEWART

Winnipeg , Manitoba Canada | 204 228 5618 | odailstewart@gmail.com

Professional Summary

Experienced and passionate Security Analyst with over 5 years of experience protecting business systems for small and large organizations.

Website: http://odailstewart.ca/

Certifications

- Microsoft Certified Professional (MCP) : ID# 16985318
- CompTIA Security+ : ID# COMP001021490629
- Splunk Core Certified Power User: ID #: 282049960
- CISM - **Certified Information Security Manager**: Pursuing*
- MS-500**: Microsoft 365 Security Administration:** Pursuing*

Skills

- HTML, CSS, JavaScript, Pyhton, Java, C++, Bash, Git
- IAM (Active Directory, Okta, Azure AD, MO365) End-user Provisioning, Group Policy
- Amazon Web Services (Lambda, Security Groups)
- Cyber Security Awareness Trainer
- SIEM (Splunk & Logrythm)
- Email Security (Google Admin, FireEye)
- Digital Shadow, Alert Logic, Ravelin,
- Fraud Watch , Blue Voyant
- End Point Protection (Cylance, Cisco AMP & Carbon Black, SentinelOne)
- Experience with MDM - Maas 360
- Working knowledge of SSL/TLS
- Good knowledge of protocols (DNS, DHCP)
- Firewall ACLs (Checkpoint, Imperva/Incapsula & Cloudflare)
- SCCM, WebEx and Remote Desktop
- MS Exchange Administration
- MS Server & O365 Administration,
- VMWare ESXI, vSphere Administration
- Vulnerability Scans and Reports (Nexpose)
- PowerShell and Linux scripting
- Project management Experience (Okta, McAfee EPO DLP / Zscaler / Maas360 / Azure)

Education

Bachelor's Degree: Information Technology

University Of The West Indies

Computer Architecture | Computer Networks | Operating Systems | Enterprise Database Systems | Software Engineering | E-Commerce | Big Data Analytics | Information Systems Security | Computer Programming

Associate of Science: Management in Information Systems

Excelsior Community College

Database Management | Web Dev | Information Systems | Computer Programming | Analysis, Design & Development

Work History

Security Analyst   08/2020 - Current

Skipthedishes

- Administer the WAF to blocks attacks, while evaluating for known vulnerabilities
- Monitors data access and activities of privileged users to identify excessive, inappropriate, and unused privileges.
- Inspects data in motion, at rest on servers, in cloud storage, or on endpoint devices.
- Monitored computer virus reports to determine when to update virus protection systems.
- Recommend improvements in security systems and procedures.
- Administer Pentesting on a scheduled basis
- Create Security Alerts (Splunk, AWS)

IT & Data Security Officer   04/2018 - 02/2020

Sagicor Group

- Okta and Zscaler admin responsible for maintaining all aspects of the end-user experience in the org.
- Monitored video surveillance feed and system alerts for suspicious activity.
- Azure IAM & IDP
- Conducted security audits to identify vulnerabilities.
- Reviewed violations of computer security procedures and developed mitigation plans.
- Monitored computer virus reports to determine when to update virus protection systems.
- Performed risk analyses to identify appropriate security countermeasures.
- Completed vulnerability scans to identify at-risk systems and remediate issues.
- Monitored use of data files and regulated access to protect secure information.
- Responsible for monitoring SIEM, DLP, Vectra, Cylance, Zscaler & Carbon Black responding to real-time threats and security incidents
- Administered McAfee epo which monitored over 2000 systems
- Provide company-wide desktop remote support for security related incidents.
- Train new employees on IT & Data security procedures and best practices

- Perform system security administration duties to resolve problems

- Perform Internal audits, vulnerability scans, and other security related tasks to identify risks

- Maintain systems in VMware EXSI lab environment

System Administrator   10/2013 - 04/2018
Ministry of Education

- Administered and maintained domain server.

- Set up accounts and workstations

- Monitor system performance and troubleshoot issues

- Train staff on new technologies

- Implemented corrective plans of action for network performance issues including availability, utilization, and latency.

Core Competencies

Operating systems: Mc OS Version 10.6, Windows 7, 8, 10(Certified), Server 2003, 2008, 2012, Exchange 2010, Linux Ubuntu, CentOS, VMware ESXI, Checkpoint

Applications: Splunk, Imperva/Incapsula, SCCM, Cisco AMP, Cylance, Zscaler, Logrythm, Carbon Black, InsightVM, Izoolabs, Alert Logic, Digital Shadow, Ravelin, Fraud Watch, McAfee Epo, Okta, Maas 360, Active Directory, O365, Microsoft Aure AD, Microsoft Word/Excel/Access/PowerPoint,