Information Security Engineer II / Incident Responder Information Security Engineer II / Incident Responder Information Security Engineer II / Incident Responder - Research OSINT Denver, CO Work Experience Information Security Engineer II / Incident Responder Research OSINT - Denver, CO February 2018 to Present Perform Incident Response, remediate, and document security events in our network such as malware, brute force attempts, IDS alerts, FireEye NX, and more. Proactive Threat Hunting for IOCs in our SIEMs like ArcSight, FireEye HX, Splunk, Kibana, LogLogic, and Microsoft Advanced Threat Analytics. Analyze FireEye triages and memory dumps with Redline and Volatility. Reverse Engineer Malware manually with REMnux/Windows VMs, or automated with FireEye AX, Cuckoo, etc., and an understanding of static and dynamic analysis. Create scripts and automate tasks with Python and PowerShell and manage some of our internal repositories with GitLab. Stop phishing campaigns and search emails with FireEye EX. Research OSINT for domains and hashes to determine if they're malicious and add indicators to MISP to check for correlations. Security Analyst / IT Administrator Broomfield, CO June 2016 to February 2018 Collaborate with our InfoSec team and penetration test our network to look for vulnerabilities and fix them. Initiate mass vulnerability scans with Nessus to search for vulnerabilities in our network. Patch our Linux systems when new CVE security alerts are sent to us through Canonical and Spacewalk. Trace suspicious emails by headers to check if they are sent from a legitimate source. Verify if sent email attachments are malicious by opening in REMnux and Windows VMs. Implement PowerShell daily with self-created modules and scripts to parse through Event Viewer for account lockouts, failed login attempts, etc. Demonstrated the scanner in MetaSploit to multiple teams so they could check if servers were vulnerable to WannaCry. Security Analyst Card Holder Data Networks - Englewood, CO February 2016 to June 2016 Contract Job) Management and consultation for clients on network security aspects for large to small businesses Analyze and respond to security threats from Firewall, Intrusion Detection Systems, Intrusion Prevention Systems, Antivirus, and other security threat data sources Configure, manage, and upgrade FW, IDS, IPS, NAC, Encryption and a wide variety of other security products/appliances Use strong TCP/IP networking skills to perform network

troubleshooting to isolate and diagnose common network problems Adhere to policies, procedures, and security practices Utilize Backbone Network Equipment such as Splunk, WhatsUpGold, Windows Servers, and IPSec VPN Concentrators Troubleshoot/Administrate LAN/WAN networks Configure, manage, and upgrade unified threat management (UTM) devices and a wide variety of other network security products (Fortinet UTMs, OpenWRT, Routers, Modems, and Cisco Switches) Prevent social engineering attacks against clients and protect their secure CDE/CHDN (Credit Data Environment/Card Holder Data Networks) Analysis of both real time and logged traffic flow to determine root causes of issues arising from unknown factors with little information Utilize Command line interfaces for FortiOS, Windows, and Linux devices Support Engineer CMIT Solutions - Denver, CO October 2013 to February 2016 Performed multiple email migrations to Office 365 and proficient with fixing backend issues with PowerShell. Deployed DirSync to synchronize on-premise Active Directory passwords with Office 365. Performed Physical-to-Virtual migrations in Hyper-V and VMware and experience supporting those environments. Experience with Exchange 2007/2010/2013 and the Exchange Management Shell. Managed Enterprise Malware endpoint solutions such as Vipre and Webroot Secure Anywhere. Responsible for maintaining backups such with ShadowProtect, Datto BDR, and Windows Server Backup. Technical Service Advisor MICROSOFT - Lone Tree, CO June 2011 to October 2013 Used MDT to deploy custom images to Surface tablets for our business customers. Provided customer service and technical support to customers with a wide range of hardware and software issues, including: Windows, Office, Mac OS's, Android, iPhone, Windows Phone and much more. Education Information Security Assurance Davenport University 2012 to 2013 Kent Career Tech Center - Grand Rapids, MI January 2003 to May 2005 Skills Penetration Testing, Forensic

Name: John Morales

Email: beverlyblair@example.com

Phone: (208)641-2767