

INFORMATION SECURITY ANALYST INFORMATION SECURITY ANALYST INFORMATION SECURITY ANALYST - MORNINGSTAR Chicago, IL Work Experience INFORMATION SECURITY ANALYST MORNINGSTAR June 2016 to Present Identify network and middleware security vulnerabilities and offer resolution advice. Use various tools such as Splunk, Qualys, Kali Linux, Sourcefire Firepower, Burp Suite, WildFire, Wireshark and many more to perform incident response investigations. Malware Analysis (Static and Dynamic) Hunt for "file-less malware" and malware that "lives off the land" Analyze logs for indicators of compromise. Monitor and respond to all incidents on 8,000 different machines. Document all Incidents at Morningstar in detail and track each until completion. Conduct risk assessments, threat modeling, privacy assessments and information security reviews on internal Morningstar systems, applications and platforms. Work directly with internal business units to communicate risk and help resolve open vulnerabilities. Monitor and manage security alerts from key information security dashboards (IDS, antivirus, centralized logging, etc.) Perform malware investigation. Automate and integrate security tools and activities. Provide security remediation advice and training to technical personnel. IT Security Analyst University of Iowa Healthcare October 2015 to June 2016 Performed incident response investigation to any malicious activity discovered or reported. Located all malware/viruses on machines and servers using BurpSuite, Sourcefire, MacAfee EPO, WireShark and performed investigations in detail after. Monitored all Firewall, DNS and Proxy logs on the network. Ran an "email Phishing" campaign to help all University of Iowa Healthcare employees better understand phishing emails. Created and updated Wiki page with tutorials on how to run each investigation. Stayed up to date on latest security trends and exploits while earning my degree. Security Engineer Intern, Trustwave June 2015 to August 2015 RFP Project Created a directory/database that can be accessed by any of the sales reps or Security Engineers (SEs) regarding questions about merchant/vendor RFP documentation. CloudShare Updates Went through the numerous CloudShare SE Environments on Windows VM's and ran system updates on all remote machines, ran updates on Java, IE, Firefox, Chrome, and any other updates that were necessary for the remote or console system to run smoothly and properly. SE Wiki Project Created and organized

SE wiki page, now the pages contains POC and Demo guides under all SE aspects so SE's can go to the page and pull the correct documentation with easy access. Spiderlabs Incident Response Intern, Trustwave May 2014 to August 2014 Shadowed forensic investigations and incident response tactics to see how they are processed. Organized confidential data and information into external hard drives for the IR team. Researched old IR cases to learn the thought process of how they were handled. Brief experience and overview with FTK and EnCase. Education Bachelor of Arts in Informatics UNIVERSITY OF IOWA May 2016 Skills It Security, Information Security, Cyber Security

Name: Chris Dennis

Email: igarcia@example.net

Phone: +1-872-410-9528x51855