|  |  |
| --- | --- |
| Christopher Ashby  **Cyber Attack Detection and Threat Response Leader** | (518) 577-8597  ashbyc@mac.com  https://ashbyca.com  PGP: [3679D138AE307F2A](https://keybase.io/ashby#show-public) |
|  | |
|  | | |
| **Summary**  Solutions-oriented, accomplished, security thought leader with proven experience participating in a broad range of corporate initiatives including architecting, implementing, and supporting information security solutions in direct support of business objectives.  A passion for solving complex security problems with proven skills prioritizing and managing multiple security initiatives with high visibility and drive results-based solutions with an emphasis on the reduction of risk while driving up resiliency within organizations.  **PROFESSIONAL EXPERIENCE**  **Senior Security Engineer, Global Security Solutions**  Alexion Pharmaceuticals, New Haven, CT, 2019–Present  Created and lead the cybersecurity threat hunting, purple team, and vulnerability programs across the organization. Acted as a threat reduction subject matter expert in various working groups to continuously drive down risk. Other key responsibilities included   * Collaboratively across the IT enterprise to resolve identified issues and/or vulnerabilities. * Implemented continuous process improvement into cybersecurity incident response tactics, techniques, procedures. * Served as a role model, teacher, mentor for security analysts, and IT workforce who weren’t well versed in cyber risk or security operations. * Work closely with the Security Center of Excellence technical team to configure, tune, and improve cybersecurity sensors, sensor settings, sensor policy configurations.   **Cyber Intel Watch Commander**  Digitalware, New York, NY, 2019–2019  Responsibilities included developing the long-term strategy and executing day to day management of a 24x7 Fusion Center environment which included a multi-faceted elite team of technology engineers, data scientists, security analysts, and threat researcher serving multiple clients across various verticals including banking, entertainment and, local state governments.   * Conducted daily strategic threat briefings for high profile customers that included in-depth threat-actor assessments, TTPs, and risk reduction remediations. * Authored and disseminated various threat notifications including, alerts, notifications, and penetration testing reports. * Maintained and managed third-party relationships including law enforcement, government officials, and vertical partners   **Director, Information Security**  CBS Corporation, New York, NY, 2013–2018  Developed and managed the threat intelligence strategy consisting of the following subcomponents providing a holistic view of the security landscape across the enterprise.  •Security Incident Event Management (SIEM)  •Vulnerability & Patch Management  •Web Application Security Management  Managed and automated the collection of OSINT & Commercial threat feeds producing operational intelligence for remote teams.  Generated and delivered routine business readiness intelligence providing an early warning of potential threats to the CBS global network and content.  Managed a team of security analysts responsible for proactively identifying threats.  Created and distributed threat metrics, advisories, and daily threat briefings that clearly articulated the security landscape to executives.  **Principle IT Security Analyst**  GLOBALFOUNDRIES, Malta, NY, 2011-2013  Work as a team lead responsible for US security operations within a manufacturing facility. General responsibilities included security operations, architecture and security solutions design as necessary to support mission critical global operations.   * Provide technical leadership to the enterprise for the information security programs and team members. * Recommend, implement and maintain, new and existing security infrastructure including IPS, Firewalls, Proxy and VPN devices. * Assess threat, risk, and vulnerabilities from emerging security issues using various organic and vendor implemented solutions including ArcSight, RSA, Bluecoat, Checkpoint, Tenable Security and Metasploit.   **Information Security Specialist**  The Active Network, Saratoga, NY, 2010-2011  Work as a security subject matter expert providing support and leadership on various company initiatives including PCI compliance testing; security architecture reviews; vulnerability discovery and penetration testing services.  **Information Security Specialist**  SAIC, Albany, NY, 2009-2010  Work as part of a team of security specialist performing various administrative forensic investigations utilizing open source and commercial toolkits including Helix v3, FTK Pro v2.x, and Sleuth Kit.  **Senior Information Security Specialist**  ReserveAmerica, Malta, NY, 2008-2009  Developed and executed various internal white-hat penetration tests against newly interconnected infrastructures and attached hosts ensuring proper mitigating security controls were in place. | **SKILLS**  Network and Systems  Operation Security  Vulnerability Management  Penetration Testing  Enterprise Security  Architecture  Incident Response  Malware Analysis  Policy and Governance  Project Management  Creative Thinking  SIEM Architecture and Management  Identity Access Management  Security Program Metrics  NIST CSF Framework  Cyber Threat Intelligence  Security Orchestration  and Automation  Employee Training  and Development  Stakeholder Management  Data Privacy  **Publications**  **PenTest Regular Magazine Pass-The-Hash Attacks Published April 2013** Article explaining the post exploitation attack technique that is used to obtain user account hashes from either client workstations or domain servers and then use this information to elevate privileges and/or create new authenticated sessions.  **PenTest Extra Magazine  Automating Malware Analysis  with Cuckoo Published August 2013** A How-To article on implementing an automated virtual environment to aid in the identification and analysis of potentially malicious software for analyst within a controlled environment.  **PenTest Regular Magazine  Extending Cuckoo Framework Published November 2013** Article describing some of the advanced features, capabilities, and extending the Cuckoo Platform. Also discusses how all the gathered analysis could be used to generate meaningful reports.  **Professional Associations**  InfraGard Member https://www.infragard.org  USCC Alum https://www.uscyberchallenge.org  Operations Security Trust https://openid.ops-trust.net  ISC – Southern CT Chapter http://www.isc2ct.org/  **Certifications**  **Certified Information Systems Security Professional - CISSP**  **Certified Cloud Security Professional – CCSP**  **Certified Information Security Manager – CISM**  **Comptia Security+**  **EC-Council Certified Security**  **Analyst – ECSA**  **ITIL v3** | |