Christopher Ashby

Cyber Attack Detection and Threat Response Leader

518.577.8597

ashbyc@mac.com

linkedin.com/in/ashbyca

Summary

Solutions-oriented, accomplished, senior security 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 projects with high visibility and drive results-based solutions with an emphasis on the reduction of risk within organizations.

PROFESSIONAL EXPERIENCE

Director, Information Security

CBS Corporation, New York, NY, 2013–Present

Joined as Lead Security Analyst, promoted rapidly through a series of increasingly responsible management positions based on strong technical, defensive security, and team Leadership performance. Currently manage 3 separate security teams within the Information Security Group.

- Developed, managed, and lead the threat response strategy providing a holistic view to the security landscape across the global enterprise.
- Provided oversight and leadership for the application security; threat intelligence; vulnerability management; and engineering teams
- Developed the various processes to source, gather, analyze and respond to cyber intelligence
- Managed a team of security analysts responsible for proactively responding to threats within the environment and delivering remediation guidelines.
- Maintained and managed third-party relationships including law enforcement, government officials, and vertical partners
- Acted as a liaison to the compliance group providing security architecture reviews of environments, platforms, and point solutions.
- Created metrics that clearly articulated the security landscape to senior executives and board members.
- Developed core security service offerings to the business to provide a mechanism for reducing risk in the environments.

Principle IT Security Analyst

GLOBALFOUNDRIES, Malta, NY, 2011-2013

Work as a team lead responsible for the USA security operations within a manufacturing facility. General responsibilities included security operations, technical troubleshooting and security solutions design as necessary to support

SKILLS

Network and Systems Operation Security

Vulnerability Management

Penetration Testing

Enterprise Security Architecture

Incident Response

Malware Analysis

Policy and Governance

Project Management

Big Data Management

Security Auditing

Identity Access Management

Security Program Metrics and Measurements

Cyber Kill Chain

Threat Intelligence

Security Orchestration and Automation

Employee Training and Development

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.

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.

- Implemented and supported security productions including software patch management; vulnerability scanning; and compliance monitoring of connected assets.
- Performed incident response and forensic investigations as needed after review of actionable events.

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.

Security Consultant

Symantec, Albany, NY, 2006-2008

Responsibilities included working in a 24x7 Security Operation Center (SOC) environment, providing analysis and trending of security log data from a large number of heterogeneous security devices. Incident Response support provided after confirming actionable incidents.

- Provided threat and vulnerability analysis as well as security advisory creation when determined applicable.
- Worked with customers both onsite and offsite to troubleshoot, reconfigure and or complete new enrollment of security devices.
- Worked with a team of security engineers performing external vulnerability scans utilizing open source software tools to discover and report potential security threats.
- Provided customers with a monthly visualization report detailing data collected from their devices which include: actionable events; web defacements; top attacking countries; and device log analysis.

Automating Malware Analysis with Cuckoo
PenTest Extra Magazine
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.

Extending Cuckoo Framework
PenTest Regular Magazine
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/

Certifications

Certified Information Systems Security Professional - CISSP

E|Council Certified Security Analyst – E|CSA

Microsoft Certified Professional – MCP

Comptia Security+

ITIL v3