# Christopher Ashby

**Cyber Attack Detection and Threat Response Leader**

(518) 577-8597

ashbyc@mac.com

https://ashbyca.com

PGP: 3679D138AE307F2A

## Summary

Highly experienced pragmatic executive, trusted advisor, and strategic problem solver taking a collaborative approach on resolving complex security problems that enable businesses to achieve their outcomes successfully across all levels of the organization.  Demonstrated success architecting, improving, and managing global cyber security related programs with a constant willingness to align and respond to the evolving threat landscape, business needs, and regulatory requirements. Confident in leading diverse teams dedicated to assessing business risks, defining appropriate mitigation, managing enterprise execution, and enhancing operational efficiency.

## PROFESSIONAL EXPERIENCE

### Senior Security Engineer, Global Security Solutions

Alexion Pharmaceuticals, New Haven, CT, 2019–Present

Created a comprehensive incident response, threat hunting, purple team, and hygiene cyber security program(s) across the organization.  Acted as a threat reduction subject matter expert in various leadership working groups to continuously drive down risk and increase resiliency across the organization.

- Collaboratively worked across the enterprise to resolve identified issues including architecture, software, and hardware weaknesses.
- Worked closely with executives on mitigation strategies to ensure the appropriate levels of risk were maintained.
- Implemented continuous process improvements for 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.

### 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 researchers 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.
- Executive level interactions in supporting city agencies C-suite particularly CISO, CSO, CIO, and CTO.

## SKILLS

Enterprise Security Architecture

Purple Team Exercises

Adversarial Emulation

Threat Hunting

Policy and Governance

Project Management

Cloud Computing

Creative Thinking

Security Program Metrics

NIST CSF Framework

Cyber Threat Intelligence

Security Orchestration and Automation

Employee Training and Development

Stakeholder Engagement

Data Privacy and Regulations

Security Risk Management

Incident Response and Mitigation

Vulnerability Management

## Education

**Harvard, Cambridge MA**
*Graduate Certificate*
2020-2020
Cyber Risk Management in the Information Age

**Ithaca College, Ithaca NY**
*Graduate Certificate*
2020-2020
Cyber Security Leadership

### Director, Information Security

CBS Corporation, New York, NY, 2013–2018

Developed and managed the global threat intelligence strategy providing visibility around enabling a holistic view of the security threat landscape across the enterprise. Managed and automated the collection of OSINT & Commercial threat feeds producing operational intelligence for remote team consumption.

- Generated and delivered routine business readiness intelligence providing an early warning of potential 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 global semiconductor manufacturing facility. General responsibilities included security operations, engineering, and security solutions design as necessary to support a mission critical global operation.

- Provided technical leadership to the enterprise for the information security programs and team members.
- Maintained, managed, and frequently engaged with third-party relationships.
- Recommended, implemented, and maintained, new and existing security infrastructure including network IPS devices, Firewalls, Proxies, and VPN appliances.
- Continuously assessed threats, risks, and vulnerabilities from emerging security events using various organic and vendor implemented solutions.

### Information Security Specialist

The Active Network, Saratoga, NY, 2010-2011

Worked as a cyber security subject matter expert providing support and leadership on various company initiatives including:

- PCI compliance testing for Level1 Merchant Accreditation
- Network Security architecture reviews and audits
- Vulnerability discovery and Penetration testing

### Information Security Specialist

SAIC, Albany, NY, 2009-2010

Worked as part of a team of security specialists performing various administrative forensic investigations utilizing open source and commercial toolkits including Helix v3, FTK Pro v2.x, and Sleuth Kit. Worked closely with NY Agency Commissioners on reducing physical security risks to both inmates and correctional officers.

### 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.

## Publications

**PenTest Regular Magazine**
**Pass-The-Hash Attacks**
**Published April 2013**

Article explaining the post exploitation attack techniques used to elevate privileges and/or create new authenticated sessions.

**PenTest Extra Magazine**
**Automating Malware Analysis with Cuckoo**
**Published: August 2013**

Article on implementing an automated technique to aid in the identification and analysis of suspicious software.

**PenTest Regular Magazine**
**Extending Cuckoo Framework**
**Published: November 2013**

Article describing some of the advanced features, capabilities, and extensibility of the Cuckoo Platform.

## Certifications

**Certified Information Systems Security Professional - CISSP**

**Certified Cloud Security Professional – CCSP**

**Certified Information Security Manager – CISM**

**Comptia Security+**

**ITIL v3**

## Professional Associations

**Ithaca College Board Member**

**InfraGard Southern CT Member**

**Operations Security Trust Member**

**ISC – Southern CT Chapter Member**