# Justin W. Hall

Veteran information security consultant

Full resume at jwhall.info

6738 Ashe Knoll
Liberty Township, OH
45011
**513.252.6011**
**jwhall@gmail.com**

## EXPERIENCE

### **CBTS,** Cincinnati, OH — *Director, Security Consulting*

MARCH 2005 - PRESENT

Over a decade consulting with the region's most successful organizations. Built SOC teams; trained and managed staff; deployed dozens of technologies; malware analysis, forensic investigation, and expert witness for federal computer crimes; vulnerability assessment and penetration testing; management, sales, budgeting, project planning and execution, hiring, team growth and strategy.

### **The Sant Corporation/Qvidian,** Cincinnati, OH — *IT Director*

JULY 2001 - MARCH 2005

Managed network for local software company. Developed foundational security controls, reduced cost, improved efficiency.

### **OneNet Communications,** Cincinnati, OH — *Tech Support Lead*

JUNE 1998 - JULY 2001

Oversaw technical support team for popular regional internet service provider. Hired and trained staff, developed user software toolkit, created knowledge base, implemented metrics and ticketing systems.

## EDUCATION

### **University of Cincinnati, Lindner College of Business** — *Bachelors, Business Administration*

GRADUATED 2004

Information Systems major, International Business minor. GPA 3.8.

## COMMUNITY

### **BSidesCincinnati** — *Co-founder, Director*

With a team of six colleagues, founded Cincinnati's first community-driven information security conference, now in its fourth year.

### **Infragard DFWG & Cincinnati Security Exchange** — *Co-founder*

Helped create and operate monthly two technical working groups, focused on digital forensics, incident response, blue team tactics, and information sharing. 3-4 talks presented per year.

## SKILLS

Vulnerability management and penetration testing

Security program development

Network security monitoring

Incident response

Managed security services

Digital forensics

Security architecture and network design

Presales & CISO strategy

Training and public speaking

## CERTS AND AWARDS

**GCIH:** GIAC Certified Incident Handler - **Gold**

**GPEN:** GIAC Certified Penetration Tester

**GCFA:** GIAC Certified Forensic Analyst

**CISA:** Certified Information Systems Auditor

**Eagle Scout,** class of 1996

## LANGUAGES

Bash, Powershell, Python

# Career Experience - Highlights

## Security Architecture

**Company SME** and evangelist for security technologies, including network defense, data protection, endpoint protection, security monitoring, and managed security services.

Led efforts to **select security products for customers**. Requirements development, evaluation/proof of concept execution, scoring and metrics.

As a consultant, designed security infrastructure, deployed to production, established operational management rhythms and processes.

**Designed and built "green field" network** for startup, with security architecture based on CIS Critical Security Controls.

## Vulnerability Management

As a consultant, **developed vulnerability management program** for large defense contractor, including vulnerability bulletin collection, prioritization and scoring based on CVSS, and remediation guidance.

**Development and management of consulting vulnerability assessment and penetration testing practice**. More than a hundred security assessments in eight years as a consultant, for large and small customers in a variety of industries.

**Four years managing consulting practice** executing more than 60 engagements a year for hundreds of customers.

Expert in ISO 27000, NIST CSF, NIST 800-53, SANS/CIS CSC.

## Security Monitoring and DFIR

**Led response efforts** for large defense contractor during investigation into APT1 intrusion in 2008.

**Performed forensic investigations,** including insider threat case for global auto manufacturer. Served as customer's expert witness for FBI case against suspect.

**Developed managed security service offering** for internal startup group. Hired and trained staff. Served as lead analyst and highest escalation point.

## Leadership

**Managed several teams** over a decade at CBTS, including a security operations team, a SOC, and a team of consultants performing assessments and design services. Day-to-day personnel management, HR, hiring and firing, promotions, and annual performance reviews.

**Vetted candidates** for internal security work, and security staff augmentation positions for customers.

Member of Cincinnati Bell security governance council, led by CISO, contributing to strategy, policy, and risk management activities.

**Managed vendor relationships,** and vetted new security technologies for resale partnerships.

## Governance, Risk, and Compliance

Executed consulting engagements covering **security program guidance and risk management** for customers in a variety of industries, including financial, healthcare, manufacturing, retail, technology, higher ed, and services.

As CBTS **security evangelist and SME**, provided strategy and guidance at CISO/CIO level for customers.

Led efforts to develop security program assessment service offering based on **NIST Cyber Security Framework** after its initial introduction.

Led efforts to develop guidance around new and updating regulatory compliance initiatives, including PCI, HIPAA, FISMA, NERC CIP, and others.

## Training & Public Speaking

**Developed custom training material**, with topics ranging from security awareness to analysis and incident investigation, and presented to customer IT and security staff.

**Regular speaker** at security community events, including Security BSides, CSX, NKU Cybersecurity Symposium, ISSA, and Infragard; security classes at four local universities; and company promotional and sales events.