



Thomas Harris

Incident Response Analyst

- Albuquerque, NM
- +1 505 485 2153
- tobraha@proton.me
- <https://tobraha.tilde.team>

About me

Information Security Specialist with 13 years of experience working in a wide range of environments supporting modern-day technology systems. Highly organized with a unique aptitude for learning and troubleshooting complex systems.

Skill

Powershell



Linux



Python



Azure



Networking & TCP/IP



AWS



Java



*This skill scale is from 0 (Fundamental Awareness) to 5 (Expert)

Document compiled with \LaTeX on May 1, 2024

-> [Source Code \(Github\)](#)

Education

- 2007-2008 Associates of Occupational Studies Universal Technical Institute
Study of Automotive Technology *Achieved 4.0 GPA and Perfect Attendance*
- 2008-2009 BMW STEP Universal Technical Institute
BMW's Service Technician Education Program ("STEP")

Certifications

- Aug. 2022 GIAC Advanced Smartphone Forensics (GASF) GIAC
Certification attained following SANS FOR585 course

Experience

- 10/23-Current Incident Response Analyst Ernst & Young
Streamline management of SIEM and SOAR with automation. Conduct incident response as required for scoped applications and workloads.
- 05/23-09/23 Security Operations Engineer Cybersheath Services Intl.
Assist clients with obtaining and maintaining CMMC and NIST 800-171 compliance. Facilitate implementation and management of security stack; build and maintain SEIM & SOAR solutions with Azure Sentinel.
- 07/16-09/23 Digital Forensic Examiner Ambitions Consulting Group
Conduct forensic investigations of servers, workstations, smartphones, and tablets. Complete processing from start to finish: evidence collection & preservation, comprehensive analysis using industry-standard tools, and detailed reporting of analysis steps and final outcome.
- 07/22-05/23 Senior Information Security Analyst Insurity LLC
Administer and utilize enterprise security tools (SEIM, EDR, Vulnerability Management, etc.) to monitor security controls and events. Identify, analyze, and report notable security incidents using current industry-standard incident response techniques and tools.
- 05/21-07/22 Senior IT Support Specialist Insurity LLC
Provide primary support for the enterprise's Windows, Mac, and Linux systems. Plan and complete internal projects, such as email and storage migrations.
- 01/18-06/19 System Administrator II Charles IT
Administration and support of client IT systems including user workstations, on-premise domains/servers and network equipment, and cloud workloads.
- 07/15-12/18 IT Systems Engineer Ambitions Consulting Group
MSP System administration for client sites of varying size and complexity. Responsible for installation and management of workstations, servers, and network equipment (firewalls, routers/switches, etc.)
- 07/11-07/15 Desktop Support Technician The Kemtah Group Inc.
From 2011-2013, provided desktop IT support at Presbyterian hospital. In 2012, I became the lead technician and managed a team of five. After 2013, worked the same role at Sandia National Laboratories.

Personal Statement

Thirteen years in this field has given me both a great wealth of knowledge and a healthy respect for the complexity and vastness of the technological landscape of today. Early on in my career, I was introduced to Linux and instantly became a fan, even though I primarily supported Windows at the time. In all these years, I've had the opportunity to get my hands on just about every type of technology that you could imagine. While I thoroughly enjoy imparting the knowledge I have gained, I am, and will remain, an avid student of this profession.