David L. Biser

Senior DFIR Lead | Forensic Specialist | Strategic Security Advisor: Cumberland, MD | 240-609-9764 | https://www.linkedin.com/in/david-biser-37875533/

Professional Profile

High-impact **Digital Forensics and Incident Response (DFIR) Leader** with over 20 years of experience spanning criminal investigations, enterprise incident response, and strategic security consulting. A veteran of the **U.S. Air Force** and a retired **Police Lieutenant**, I bring a unique "street-to-server" investigative intuition to complex cyber breaches. Proven track record in leading high-stakes ransomware remediations, testifying as an expert witness, and building regional forensic capabilities from the ground up.

Core Expertise

- **Incident Response:** Ransomware Recovery, BEC Investigations, EDR/MDR Management, Threat Hunting.
- **Digital Forensics:** Dead-box & Live Response, Artifact Analysis (MFT, Registry, AmCache), Expert Witness Testimony.
- **Strategic Leadership:** vCISO Advisory, Tabletop Exercise (TTX) Design, Policy Development, SOC Mentorship.
- **Technical Education:** Adjunct Instructor for CEH, Ethical Hacking, and Incident Response.

Professional Experience

RedHelm | *Digital Forensics and Incident Response Lead* | **Oct 2021 – Oct 2025**

- **Breach Leadership:** Spearheaded complex investigations involving ransomware and Business Email Compromise (BEC), coordinating between legal teams, insurance carriers, and technical restoration squads.
- **Forensic Mastery:** Conducted deep-dive examinations using **EnCase, Magnet AXIOM, and Autopsy** to identify root cause and data exfiltration markers.
- **Enterprise Triage:** Leveraged top-tier EDR tools (**CrowdStrike, SentinelOne, Carbon Black, MS Defender**) to hunt threats and contain active infections across diverse customer environments.
- **Advisory:** Served as a **vCISO** for mid-market clients, designing vulnerability management programs and custom tabletop exercises to mature their security posture.

Solis Security | *Incident Response Analyst* | **2020 – 2021**

- **Rapid Response:** Acted as a primary responder for third-party incidents, specializing in O365 intrusion analysis and evidence preservation.
- **Advanced Artifact Analysis:** Utilized specialized toolsets (**CIDR, MFT tools, Registry reviews**) to reconstruct attacker timelines in high-pressure environments.

Iron Mountain | *Incident Response Engineer* | **2017 – 2020**

- **Internal Threat Defense:** Managed in-house digital investigations for a global information management leader, focusing on G-Suite and O365 security.
- **SIEM Operations:** Monitored and triaged enterprise-level alerts using **QRadar**, drastically reducing time-to-remediation for internal incidents.

Cumberland City Police Department | *Lieutenant / Criminal Investigator* | **Retired**

- **Forensic Pioneer:** Designed and implemented the first dedicated computer forensics lab in Western Maryland.
- **Expert Witness:** Qualified and testified as a technical expert in **Federal and Circuit Courts** regarding digital evidence.
- **Leadership:** Promoted through the ranks to Lieutenant, overseeing criminal intelligence and multi-agency investigations.

United States Air Force | *Sergeant / Security Specialist* | **Prior Military Service**

- Ensured high-level security for flight line operations and storage facilities; developed the foundational discipline and vigilance required for high-stakes security work.

Technical Toolkit

- **DFIR Tools:** Magnet AXIOM, EnCase, Autopsy, FTK Imager, CDIR, KAPE.
- **EDR/SIEM:** CrowdStrike, SentinelOne, Carbon Black, MS Defender, QRadar.
- **Vulnerability/Threat Intel:** Nucleus, VulnCheck, VirusTotal, Any.Run.
- **Investigations:** Malware Triage, Log Aggregation, Network Forensics.

Specialized Training & Certifications

- **EC-Council:** Certified Ethical Hacker (CEH), Computer Hacking Forensic Investigator (CHFI), Certified Network Defender (CND), **EC-Council Certified Security Analyst (ECSA).**
- **IACRB:** Certified Penetration Tester (CPT).
- **Federal Training:** Basic Computer Evidence Recovery (**U.S. Secret Service**).
- **Professional Development:** Dale Carnegie Skills for Success.

Education & Community Impact

- **Adjunct Instructor:** Teaching Computer Forensics and Ethical Hacking at the collegiate level.
- **Family Crisis Resource Center | Network Security (2014–Present):** Providing dedicated security oversight and data protection for this social services organization to ensure the integrity and privacy of sensitive information.
- **Security Researcher:** Author of technical bulletins and security blogs focused on emerging threats.