Bryan Barnhart – Digital Forensics & Incident Response Consultant

GIAC Computer Forensics Analyst, GIAC Penetration Tester

954.779.6355
bryan@infiltrationlabs.com

Summary:

Bryan is a seasoned cybersecurity expert with over 20 years of experience in both public and private sectors. His expertise encompasses:

- Digital forensics and hacking investigations for businesses ranging from small enterprises to Fortune 500 companies
- Mobile digital forensics and examination of smartphones, tablets, and other mobile devices
- Supporting attorneys with electronic evidence matters, including expert witness testimony and case consultation
- Insider threat investigations and incident response planning
- Vulnerability assessments and Red Team engagements
- High-profile investigations including data breaches, corporate hacks, identity theft, child exploitation, and fraud
- Training law enforcement and private organizations in cybersecurity, digital forensics, and investigations
- Curriculum development and instruction, including:
    - Redesigning and instructing the U.S. Secret Service Network Intrusion Response (NITRO) course at the National Computer Forensic Institute (NCFI) from 2016 to 2019
    - Teaching Digital Forensic Evidence for Florida judges at the Advanced Judicial Studies conference
    - Developing courses on Digital Forensics and Incident Response for Law Enforcement

Experience:

Owner/Operator, Infiltration Labs, LLC
Founder & Principal Consultant
August 2016 - Present

- Infiltration Labs is a cutting-edge information and cybersecurity consulting firm specializing in Digital Forensics Incident Response (DFIR) and Offensive Security Services. Key responsibilities and achievements include:
- Conducting digital and mobile forensics, hacking investigations, and insider threat analyses
- Leading ransomware/malware response and email compromise investigations
- Providing offensive security solutions including penetration testing, social engineering, and insider threat simulations

- Offering Virtual Asset Trace and Recovery Assistance for cyber fraud victims
- Overhauling and instructing the U.S. Secret Service's Network Intrusion Response (NITRO) course at the NCFI (2016-2019, 2024-Present)
- Developing and delivering specialized courses on cyber fraud, internet investigations, cybersecurity, digital forensics, and incident response for various sectors

Incident Response Consultant, Dell SecureWorks
February 2015 - August 2016 (1 year 7 months)

- Led PCI Forensic Investigations and insider threat/malicious employee investigations
- Conducted network intrusion response and mobile forensics
- Developed and tested Computer Security Plans
- Facilitated Incident Response workshops and Tabletop exercises

Security Consultant, Trustwave SpiderLabs
April 2013 - February 2015 (1 year 11 months)

- Performed digital forensics and incident response for high-stakes cases involving theft of cardholder data, banking credentials, PII, and unauthorized access
- Conducted advanced Social Engineering assessments using phishing and telephone-based attacks

Network Intrusion Incident Responder / Digital Forensics Examiner, United States Secret Service
2010 - April 2013 (3 years 4 months)

- Investigated a wide range of cyber-crimes as part of the Miami Electronic Crimes Task Force
- Specialized in computer crimes, network intrusions, data breaches, fraud, and wireless exploitation

Police Detective, City of Fort Lauderdale
June 2002 - April 2013 (10 years 11 months)

- SWAT Team: Served as Instructor, Entry Operator, Explosive Breacher, and Tactical Electronics SME (2004-2012)
- Cyber and Economic Crimes Detective (2006-2013): Focused on identity theft, fraud, and cybercrime investigations

Security Operations Center Manager, Cyberlynx/WebUnited
June 2001 - June 2002 (1 year 1 month)

- Managed a team of security analysts, developers, and engineers
- Developed Linux shell (sh, csh, bash) and PERL scripts to automate QA tests and streamline daily operations

- Administered over 50 Firewall/IDS boxes across multiple platforms, providing 24/7 intrusion detection and blocking
- Built, configured, and installed ProtectPoint Systems (Firewall/IDS)
- Conducted vulnerability assessments on customer networks
- Analyzed and responded to network intrusions, updating IDS and Firewall Rules accordingly
- Maintained and updated MYSQL databases

Systems Administrator, Cybergate/ValueWeb
June 1998 - June 2001 (3 years 1 month)

- Installed, configured, and maintained mission-critical client-server systems
- Troubleshot and resolved system issues including FTP, DNS, HTTP, POP, and SMTP servers across Linux, AIX, and BSDi platforms
- Managed software installations, new releases, upgrades, and supporting products to ensure optimal system performance

Fire Team Member, United States Army, 1st Ranger Battalion 75th Regiment
1994 - 1996 (2 years)

- Served as a member of an elite special operations light infantry unit
- Developed strong leadership, teamwork, and problem-solving skills in high-pressure environments
- Participated in rigorous training and missions, enhancing physical and mental resilience

Technical Training

Linux Attack & Detection	2024
Investigating Windows Endpoints	2024
Rapid Ransomware Response	2023
Enterprise Digital Forensics	2023
Data Breach Investigation and Response	2020
Battlefield Forensics	2019
Digital Forensic Evidence for the Courtroom for Judges (Instructor)	2019
United States Secret Service Network Intrusion Investigations (Instructor)	2016 - 2019
SANS Network Penetration Testing and Ethical Hacking (GPEN)	2016
Certified Information Systems Security Professional (CISSP)	2015
SANS Advanced Computer Forensics Course (GCFA)	2015
Payment Card Industry Qualified Security Assessor (PCI-QSA)	2014
Basic Network Intrusion Investigations (Proctor)	2012
Point of Sales Systems Investigations (Proctor)	2012
NCFI Point of Sales Systems Investigations	2012
Financial Fraud Investigations	2012
Immunity Inc. Web Hacking Techniques	2012
DOD DC3 Digital Forensics Examinations	2012
DOD DC3 Cyber Law & Ethics	2012

DOD DC3 Cyber Crimes Investigative Process	2012
SRT WiFi Investigative Techniques	2012
SRT WiFi Exploitation/Hacking Techniques	2012
SRT Router Interrogation Techniques	2012
SRT Tracking Suspects via Wi-Fi	2012
TLO Child Protection System/ForensicScan	2012
USSOUTHCOM Cyber Counter Intelligence Conference	2012
Infiltrate2012 Offensive Security Conference	2012
Facebook 201: Tools, Tricks and Techniques Investigators need to know (webinar)	2012
FTK ACE	2011
Basic Cell Phone Investigations	2011
Basic Computer Evidence Recovery Training	2011
Computer Forensic Investigations	2011
Forensic Cell Phone Data Recovery	2011
GPS Forensics Investigations	2011
Tactical GPS Forensics Technology	2011
Advanced File Structure Analysis	2011
Criminal Interview and Interrogation Techniques	2011
Decoding Digital Evidence (webinar)	2011
Mobile Device Tracking	2011
Cell Phone & Portable Storage Device Forensics	2010
DefCon18	2010
Role of Covert Technology in Mumbai Attacks	2010
Enterprise Investigations Involving Packet Capture (webinar)	2010
On scene Computer Forensics and Digital Previews (webinar)	2010
Online Social Media and Investigations (webinar)	2010
Search & Seizure in the Electronic Age	2009
Cell Phone Technology	2009
3SI Security Systems: Electronic Satellite Pursuit Currency Tracking	2008
Kinesics Interview	2006
Linux Systems Administration	1999
Linux Network Administration	1999