TREY BLALOCK

GWAPT, GCFA, GPEN, CISA, CISM, CRISC, CISSP, SSCP, NSA-IAM

Address : 3518 Fremont Avenue North, Unit # 186 Seattle, WA 98103-8814 /E-mail : trey@firewallconsultants.com/Phone : 404.550.8739

HIGHLIGHTS

Served as Manager of Global Security Operations / Security Architect for one of the worlds largest financial transaction hubs (S1 Corporation) overseeing all aspects of security for hundreds of web-banking environments, ATM networks, and point-of-sale transaction networks world-wide.

Designed, deployed, and secured many complex AWS-based cloud architecture solutions for large organizations including Best Buy, Carhartt, CenturyLink, Toys-R-Us, Walgreens, Target, McKesson (Canada), Harrods (UK), Sainsbury's (UK), Car Phone Warehouse (US), M. Video (Russia), and T-Mobile.

Has served as a Computer Forensic Expert Witness for the U.S. Department of Justice on multiple cases including handling all aspects of computer forensics on some high profile cases such as "Donald Vance vs. Donald Rumsfeld", "John Doe vs. Donald Rumsfeld", and "American Boat Company vs. United States".

Has trained numerous Fortune 100 companies, consulting firms, and federal agencies such as the FBI, NSA, and DIA on network security, system security, attack & penetration testing, and cloud security.

Has over ten years of experience providing penetration testing and assessment services to hundreds of clients in the financial, government, retail, chemical, oil & gas, medical, educational, legal, telecom, and law enforcement sectors.

Has served on several security related advisory boards including the National Board of Information Security Examiners (NBISE) Operational Security Testing Panel, the SANS GIAC Advisory Board and previously the National Security Telecommunications Advisory Committee (NSTAC) for the Government Emergency Telecommunications System (GETS) research and development working group.

Writes and teaches attack & penetration testing classes and speaks on topics such as big data security, cloud security and security automation.

EMPLOYMENT HISTORY

Verification Labs, LLC
January 2014-Current

Lead Penetration Tester / CISO / Founder

Created a company specializing in advanced penetration testing and security audits. Verification Labs has been providing a variety of different services including conducting PCI-DSS control assessments, a wide variety of infrastructure and application penetration testing for organizations of all sizes, has performed advanced red team engagements, spear-phishing campaigns, large-scale security assessments for multi-billion dollar companies, and has conducted public and private penetration testing classes.

T-mobile via UST-Global
October 2015-March 2016

Principal Security Architect (sub-contract via Firewall Consultants)

Designed PCI-DSS 3.0 based security architecture controls and related solutions for AWS platform hosting thousands of EC2 instances. Designed system for automatically taking forensic images of EC2 instances and a large-scale system for automatically blacklisting attackers IP addresses based on a variety of different events. Served as subject matter expert on several different technologies.

EMPLOYMENT HISTORY CONTINUED

Confidential
/Security Startup
April 2015–October 2015

Vice President Security Solutions

Designed a large-scale supply chain surveillance product to remotely evaluate the security of vendor networks. This system involved combining a mixture of attack & penetration techniques, building several Internet-scale reconnaissance tools, integrating data from dozens of unique IP reputational systems, dark-web information sources, and threat intelligence products then combining the results from these findings into an easy to use web portal with a customizable scoring and alerting system.

Tier 3 / Century Link Cloud
via Apex Systems Inc.
November 2014–April 2015

Security Engineer (Contract)

Developed unique Internet-scale security automation solutions for a cloud-compute provider. Details are restricted due active non-disclosure agreement.

T-Mobile via Experis
June 2012–August 2013
and also Mar 14–Nov 14

Systems Security Design Engineer (Contract)

Designed the security controls for some of T-Mobile's largest and most complex projects including the creation of custom security solutions to meet regulatory requirements for CPNI, PCI, SOX, PII, and special Department of Justice requirements. Specifically, I managed all aspects of security for several projects including the creation of security requirements, updates to T-Mobile's security policies, and the creation of security documentation, SDLC security lifecycle integration, security escalations, and management of requirements for third-party vendors. Served as a subject matter expert for the following areas: compliance, cloud-computing, high-performance computing, storage security, IPv6 security, mobile device security, vendor security assessments, legal security issues, incident response techniques, host-based security controls, application security controls, and penetration testing methods. Served as the internal penetration tester for several projects including T-Mobile's MetroPCS PCI audit.

Pfizer via Mphasis
August 2013–March 2014

Penetration Testing Expert (Contract)

Has recently conducted over 100 manual penetration tests against major Pfizer web assets for well-known drugs such as Advil, EmergenC, Viagra, ThermaCare, Pristiq, Nicotrol, and Zoloft. Have also conducted many application penetration tests against critical business applications and third-party business partners. Testing has included sites in a wide variety of languages including French, Spanish, Portuguese, Mandarin, Japanese, Russian, Swedish, Norwegian, German, Arabic, and Hindustani and across a very wide variety of web platforms hosted around the world. Through this process, I have manually verified a very wide range of security problems, documented how to replicate the exploitation manually, and then provided support and training to development teams to remediate the problems found. Additionally, I have also served as a subject matter expert for several other security teams.

State of Wisconsin
via KForce
June 2011-Nov 2011

Redesigned Network Security Architecture (Contract)

Redesigned the entire network security architecture for the State of Wisconsin including all data centers and all agency interconnects. Trained staff on advanced high-availability architecture techniques, security architecture, and security engineering. Designed network security controls to protect the State of Wisconsin's primary mainframe computer at this location. Managed the entire project and coordinated communications between all related agencies and departments to make the project a success. Frequently helped troubleshoot advanced networking problems and developed network monitoring solutions to prevent future problems in addition to the primary project responsibilities.

Predictix, LLC.
Sept 09-June 11

Manage All Aspects Enterprise Security

Managed all aspects of enterprise security, cloud computing security, penetration testing, vulnerability scanning, SIEM deployment, and legal contract review for a company handling data for some of the largest retail companies in the world including Best Buy, Walgreens, Toy's-R-Us, Sainsbury's (U.K.), and M.Video (Russia). Handled all aspects of security for this company and served as the subject matter expert for all network and performance related issues. Additional details are available upon request (note: some aspects of the technology used here are confidential).

EMPLOYMENT HISTORY CONTINUED

S1 Corporation

Sept 08-Sept 09

Manager of Global Security Operations / Security Architect

Managed all aspects of S1's global security operations other than internal audit, which operated as an independent team. S1 Corporation is the world's largest financial transaction hub, which allows many of the world's largest banks, retailers, credit unions, and processors to connect to each other for payment processing. With over 3000 companies around the world, including many well-known companies such as Bank of America, McDonald's, the Pulse Network, PayPal, and Wells Fargo, as clients I have managed to work directly with a very large percentage of the world's largest and most demanding financial entities. During this time I served as the sole security architect for all security projects and customer implementations as well as created and managed several security teams handling all aspects of security including the following: enterprise security; physical security; video cameras; data destruction services; private security services (building security guards); evidence rooms; safes; biometric readers (hand scanners); complex RSA PKI infrastructure; IDS/IPS; Firewalls; VPN; network infrastructure; advanced load-balancing architectures, multiple authentication systems; SEM/SIM's (QRadar); Incident Response Team; Forensics; interfacing with law enforcement; being the main point of contact for customer incidents; media control; security architectural board approvals; security change controls; securing multiple PCI environments; handling PCI, FFIEC, SAS70, and customer mandated audits; vulnerability scanning of over 70,000 IP addresses worldwide; penetration testing on major banks; application scanning of proprietary applications; installation of application layer firewalls (Imperva); security awareness training; technical training; internal and external presentations; etc...

In addition to my management and security architecture roles I also served as the primary incident responder/forensic analyst/law enforcement interface for all incidents involving financial loss and also served as a subject matter expert for several non-security teams on subjects such as advanced protocol analysis (including analysis of proprietary ACH implementations) and advanced system administration and system performance issues. From an auditing perspective, I managed to reorganize the collection of all data into a single ISO27002-based set of containers so that all future auditing information could be gathered from a single location regardless of the audit type

Forensic Response International, LLC.

June 04–Sep 08

Forensic Expert

Founded Forensic Response International, LLC. a company with a primary focus on handling live incidents and compromised systems. Forensic Response International, LLC. has provided a wide-range of clients such as the U.S. Department of Justice, The University of Georgia, S1 Corporation, Southern Company, AIG, Accenture, and SunGard with forensic and data recovery services. I have provided expert witness services including writing subpoena's, providing forensic services, handling evidence, and testifying in federal court for the U.S. Department of Justice on a number of cases including Donald Vance vs. Donald Rumsfeld and American Boat Company vs. United States. I have also handled multiple forensic cases involving on-line bank robberies against large banks such as Bank of America. In addition to incident response programs I have created for S1 Corporation and EarthLink (see below) I have created incident response programs for various organizations and large global corporations such as AIG.

Another area where I have done considerable work in is training security teams on a variety of forensic-related subjects including Electronic Discovery; legal issues involving forensics; forensic analysis of live systems; forensics on PDA's, cell phones, and other electronic devices; advanced use of forensic tools and specialty searches; and legal issues involving expert reports, depositions, and testimony. Additionally, I have built a large forensic lab, which has an extensive collection of forensic tools for imaging and analyzing a wide variety of devices, and have multiple forensic workstations for handling multiple investigations simultaneously. I also have provided data recovery services for numerous hard-drives, RAID arrays, digital cameras, USB Flash Drives, and PDA's.

EMPLOYMENT HISTORY CONTINUED

Firewall Consultants, LLC.

July 03-Current

Internet Security Specialist / Penetration Tester

Founded Firewall Consultants, LLC., a managed security service and consulting organization. While working at Firewall Consultants, I've configured or worked in almost one hundred different complex environments installing or reconfiguring firewalls, load balancers, switches, VPN's, and routers, most of which have had very advanced high-availability setups. I've provided numerous companies with emergency troubleshooting services, normally involving the use of protocol analyzers, to resolve network, system, and application problems. My troubleshooting services are frequently resold by consulting companies and ISP's such as SunGard Availability Services where I work on behalf of their support team to troubleshoot some of the most complex problems which their internal staff cannot resolve or when a serious emergency has occurred. In addition to support services, I've also hired developers to help me produce a highly customizable managed vulnerability scanning appliance/service. I created this service so that it would be scalable for very large enterprises (400,000+ IP's) but also affordable for smaller companies and non-profits, especially ones needing to comply with current regulatory compliance standards. Additional work performed includes having conducted multiple ISO-17799 based security audits (pre ISO-27001), I have developed, and currently run a managed firewall service for multiple clients in SunGard's 1055 Spring Street data center (formerly Inflow) which also happens to be our primary data center (tour of our equipment at this facility upon request). In 2005 I began rebuilding NPR's Content Depot network architecture, this included a complete redesign of the network and installation of network monitoring / performance monitoring services. I recently have also completed a large-scale network re-design for Multicast Media Networks a streaming video service provider that services over 700 channels of 24x7 streaming video. Firewall Consultants has also performed penetration testing against a very wide range of equipment including small IoT devices, mobile apps, mainframes, and large-scale cloud deployments for Fortune 500's. Most recently Firewall Consultants spent ten months helping Apple Leisure Group conduct penetration testing, vulnerability scanning, prepare for PCI audits, and develop security processes for their production operations.

S1 Corporation

May 06–November 06

Security Analyst #3

I was originally brought in as a Forensic Response International consultant to triage some production banking servers which had been compromised and were still being used by attackers as a location to further their activities. Shortly after that contract began S1 negotiated a long-term part-time package to allow me to train their staff and help build an incident response center as an employee. In this role, I served as a subject matter expert in a variety of security and networking areas and was a strategic resource for forensics and troubleshooting. Another large part of my duties included handling many aspects of internal assessments and formal audits by external parties, such as the FFIEC.

Earth Link Corporation

November 02–July 03

Information Security Analyst

EarthLink originally hired me as an Information Security Analyst within their newly formed IT Risk Department to handle complex incident response tasks that couldn't be addressed by their network security and abuse departments. My duties included computer forensics, developing short-term and long-term Incident Response Systems, finding and resolving large-scale security issues unique to EarthLink's proprietary internal systems, and interfacing the with the media. Some specific issues I've dealt with include preventing Wired media from doing an article on a large-scale problem EarthLink had, organizing our legal department and vendor representatives to force one of our business partners to stop allowing the problem and creating tools to fix the systems damaged by one of our vendors which could have affected thousands of customers. Additionally, I performed computer forensics on systems that had been compromised, trained staff on specific firewall and VPN architecture problems. Performed security assessments on critical servers and wrote the EarthLink corporate security policy. I was also the EarthLink representative for the National Security Telecommunications Advisory Committee (NSTAC), which dealt with the research and development of the next generation Government Emergency Telephone System (GETS).

In April 16th 2003 in an effort to spend more time doing forensics and IDS work, I transferred to the Enterprise Network Security team as a Senior Security Engineer. In this new role, I was still doing all of the forensics on compromised systems and still the primary technical contact for all major incidents, but was also responsible for deploying and administering the Cisco IDS's, and as a secondary role helping to administer the 140 FreeBSD IPFilter Firewalls, some of which had over 40,000 rules. I also developed the process for monitoring wireless security activity and vulnerabilities across all EarthLink locations.

Buffalo Rock Company
October 02–November 02

Security Assessment (Contract)
Communication Network Corporation in Birmingham, Alabama contracted me to do a security assessment for Buffalo Rock Company a Pepsi-Cola Bottler with 13 different distribution centers headquartered in Birmingham Alabama. I conducted an ISO-17799 based network security assessment on over 600 hosts across all 13 corporate locations. This assessment involved extensive analysis of all routers, switches, Firewalls, VPN's and an analysis of the modem connections in their primary Datacenter. While on-site I was also able to spend time training their staffs on how to re-design their Firewall/VPN architecture to more effectively secure their network. Additionally, I was able to help the customer by discovering problems in a wide range of areas including DNS configuration problems, Syslog anomalies, wireless security issues and a variety of physical security problems.

Alliance Coal
July 02-Current

Forensic Analysis + Security Assessment (Contract)
GDH Consulting in Tulsa, Oklahoma contracted me to do a combined forensic analysis on an AIX server (confidential) and a basic security assessment (non-ISO17799 due to customer time/financial constraints) for Alliance Coal. I discovered and was able to determine the exact details of what happened on their server (confidential) and was able to give a detailed report with my findings including a list of all files affected, the exact time and duration of the event, and a systematic description of exactly what took place. I also was able to do an ISO17799 based network and system security audit, which uncovered some very interesting (confidential) findings. While on-site I also spent time training the Alliance Coal engineering team on the "bit-level" details of how attacks work and taught them many advanced security tricks that solve complex architectural security problems. I wrote an executive report documenting my findings and many recommendations as well as the order in which Alliance Coal should begin working on the recommendations I laid out. Alliance was so pleased with my work that their engineering team sent me a thank you letter and a gift after I was finished.

Omnexus
December 01–July 02

Security Specialist (Contract)
I contracted as a Security Specialist overseeing all aspects of security at Omnexus Americas Inc. Omnexus runs an on-line marketplace, which allows customers to make transactions from large plastics suppliers such as BASF, Dow Chemical, and DuPont. I was responsible for all of the VPN's connecting the ERP's between their suppliers and their e-marketplace, as well as those used for the Internal connections between their U.S., European offices and remote users. I also managed the Checkpoint and Pix Firewalls, Cisco routers, switches, F5 BigIP's, and Snort IDS's on the production network. In addition to these responsibilities, I created a secure Intranet using multiple Linux boxes running Apache, Mod_ssl, MySQL, a variety of Perl based security tools and web-based network management tools to keep track of performance tuning statistics for all of the equipment and applications in Omnexus's production environment. I conducted weekly security scans, re-wrote the company security policy, helped fix all the major security holes on the internal and production networks, and fixed many of the system and network problems Omnexus had been having on both their networks as well as those of some of their business partners.

AT&T, Network
Professional Services
August 01–November 01

Security Specialist (Contract)
My primary duties at AT&T included training AT&T's senior security consultants on how to perform advanced security audits and penetration tests; these were conducted on customer premises for some of AT&T's larger international customers. Part of my duties also included setting up advanced firewall and IDS architectures in AT&T's labs in order to help train their staff on some of the solutions to the more complex problems involving firewalls and IDS's. Additionally I also did some network and system consulting on behalf of AT&T for some of their global accounts, as well as helped develop and demonstrate potentially new service offerings for AT&T's managed Intrusion Detection service.

EMPLOYMENT HISTORY CONTINUED

State of California
Franchise Tax Board
June 01–July 01

Security Audit (Contract)

The director of the University of Southern California's Center for Information Assurance Studies hired me to conduct an ISO 17799 based security audit of the State of California's Franchise Tax Board (FTB) as well as to analyze some specific security architecture problems involving their OS/390 systems. FTB electronically transfers over 42 billion dollars per year into a very complex network containing over 5000 computers, hundreds of proprietary applications, almost every imaginable operating system, hundreds of dial-up lines, and a 24-node remote site frame-relay mesh. I managed to accomplish all of the on-site auditing tasks by myself over a three week period well ahead of the 5-weeks that had been originally planned for the project by USC. Additionally during this audit, I found major vulnerabilities on almost every networked device as well as major design flaws in their network architecture, router and switch configurations, electrical systems, air-conditioning systems, power generation systems, employee screening process, access-control systems, CCTV systems, mainframe deployment, etc. In addition to these findings, I spent time teaching FTB's staff how to analyze their security systems themselves and helped re-design their network architecture to create a much more secure network environment. I also made many detailed recommendations on how to help secure their individual Windows, Unix and OS/390 environments.

Blue Storm
Jan 01–May 01

Principal Security Consultant (company closed)

I was a Principal Security Consultant doing security consulting for Fortune 100 companies and government agencies. I was the primary subject matter expert for security architecture, firewalls, penetration testing, and computer forensics. Some of my internal duties included creating the course material used to train all of the other security consultants and creating a baseline for determining what a consultant must know to do a particular job as well as giving the final approval for most of the security team hires nation-wide. Customer-oriented duties included: penetration testing, high-availability firewall implementation, wireless security architecture, speaking at conferences, sales engineering, writing security policies, developing BS7799 / HIPAA / GLBA based audits, designing and deploying complex security architectures, supervising security engineers, developing proposal and pricing documentation, development of PKI, LDAP and Secure ID installation procedures and development of penetration testing tools.

Netsentinel
July 00 - Dec 00

Sr. Director, Managed Security Services and Countermeasures

I was managing three product development teams, was the lead auditor / professional security services specialist and had a direct involvement in all aspects of business development in both the U.S. and Europe. The teams are listed as follows:

Network Security Services Group – This group did not exist before I came on board and was formed to create the following managed security services; Managed Firewall Services, Managed Intrusion Detection Services, Managed Virus Scanning/Malicious code services, and Managed VPN services. All of these services became operational with the exception that the Managed Intrusion Detection Service had to be in one of our Secure Operation Centers until the remote product was completed.

Physical Security Group – This group had previously been using Northern Computers hardware and WINPAK software to integrate multiple types of access control devices, including several types of biometric authentication devices and CCTV cameras, into a basic managed access control system. We moved this product to a redundant embedded Linux solution, which allowed us to exceed the original hardware and software limitations as well as allowing us to integrate the records from the controls and also giving us the ability to take snapshot images from the cameras into a customer viewable web page which we planned on integrating into our managed security services product. I also had this group design a formal physical security audit procedure and the appropriate documentation to integrate into our security audits.

Security Audit Team – This is another group I was hired to create. Previously all customer security audits had been outsourced to Ernst & Young due to lack of appropriate personnel on staff to do such tasks. Having formerly trained a large number of Top 5 Consulting firms while working at Learning Tree it was very easy to create an audit that went far beyond the formal security audits which consisted primarily of running off the shelf scanners and a handful of free tools to scan only the IP aspect of their customer's networks. To take our audit beyond what many companies have been doing I trained my staff how to analyze and penetrate various legacy and proprietary protocols as well as how to handle the auditing of non-standard network equipment. Specifically I taught them exactly how various systems, routers, and switches could be broken into or compromised and exactly what needed to be done to avoid such problems. Many of these problems are inherent in the design of some networks and network devices and cannot be detected with off the shelf security scanners and are not usually caught in audits. This is also the same team I was using to create a professional services group with.

In addition to managing these groups I also did a lot of professional services work that was network oriented but not security related, specifically I had been working at City Reach International's Amsterdam and London facilities to help with their network design and peering which are currently being deployed across 20 countries connecting their data centers as well as all of the telecommunications providers and ISP's within their data centers.

Eattorney.com
June 99–May 00

Director, Network Security

Designed and installed a fully redundant network using Cisco 3640's, Cisco Catalyst 3524's, Checkpoint Firewall-1's, F5's Big IP, and F5's 3DNS product. Deployed NMLI network to connect office to co-location centers along with dual T1's for back up. Installed custom Sniffer scripts on dedicated Sniffers at every wan interface as well as internally on development LAN. Integrated Big brother, Tripwire, arpwatch, and Multi-Router Traffic Grapher into the environment to monitor network and page respective administrators. Managed a small IT group to run all internal operations. Secured all "production" equipment at co-location sites. Wrote disaster recovery plan and security policy.

Learning Tree International
June 97-January 00

Senior Instructor

Taught public and custom courses on Firewalls, Unix Security, Cisco routers, TCP/IP, and IPv6. I was the lead instructor for all Firewall classes taught worldwide for three years and was responsible for training other instructors on the Firewall courses as well as responsible for teaching all custom Firewall courses.

The bulk of the clientele for these courses were Federal agencies including the U.S. Army CERT team, U.S. Navy CERT Team, FBI Computer Forensics team, U.S. National Security Agency, Canadian National Defense, U.S. Naval Surface Warfare Group, Defense Information Systems Agency as well as many Fortune 100 security specialists and auditors. In March 2000 I was offered to write Learning Tree's Intrusion Detection Course however due to conflict with work at Eattorney.com I opted to be the technical editor instead. Many additional references are available upon request.

Hewlett Packard
June 96–June 97

Response Center Engineer

Worked as the lead support engineer for all A and B level military security products including BLS, CMW, and all Virtual Vault products. I was part of the HP staff on the code-review board dealing with the National Security Agency's certification review for CMW. I was also on the modified kernel support team, which supported all Unix performance tuning tools such as Glance, Measureware, and Netmetrix on multi-processor systems, and worked closely with the core-dump analysis team on issues involving crashes on modified kernel systems. Although my primary responsibilities were to support products from the Federal Computing division of HP I was frequently given many of the "live" security incident calls that came in through the response center for traditional HP-UX

MAPICS Inc.
June 95–June 96

Senior Network Administrator

Completely designed, supervised, and implemented Mapics Inc.'s Token-ring to Switched Ethernet conversion which included over 3000 nodes in 28 countries. I was also responsible for upgrading Mapics Inc.'s 28-country X.25 network to a combination of Frame-Relay, dedicated T1/E1's and fractional T3's. Planned, documented, and executed a conversion to RFC 1918 IP addressing for all internal addresses for Mapics Inc. global operations, the entire conversion, including all modifications to databases, mail-servers, X11 configurations, NFS/SMB shares, AS/400 applications and custom internal applications was executed successfully in less than 70 minutes. Installed and maintained PIX Firewalls for all offices and setup VPN's to connect all remote offices. Duties also included system administration of HP9000, IBM RS/6000, AS/400, and OS/2 based servers.

RELATED CERTIFICATIONS

- GIAC GWAPT
  (Global Information Assurance Certification) GIAC Web Application Penetration Tester # 3845
- GIAC GCFA
  (Global Information Assurance Certification) GIAC Certified Forensic Analyst # 355
- GIAC GPEN
  (Global Information Assurance Certification) GIAC Certified Penetration Tester # 2089
- CISA
  Certified Information Systems Auditor # 0862743
- CISM
  Certified Information Systems Manager # 0910809
- CRISC
  Certified in Risk and Information Systems Control # 1620233
- CISSP
  Certified Information Systems Security Professional # 11246
- SSCP
  System Security Certified Practitioner # 23259
- NSA-IAM
  National Security Agency Information Assessment Methodology certified as of 09/13/02