Travis B. Green

Missoula, MT • travis@travisgreen.net • (406) 284-1911 • travisgreen.net • linkedin.com/in/travisgreen

Passionate Cyber Security researcher and consultant with a 20-year career that includes extensive international work leading security initiatives, advising government and military clients, consulting to enterprise businesses, and mentoring teams in best practices. Effective communicator and self-starter able to analyze data to create security policy, develop and execute strategy, and develop tools to automate processes. OISF core team member with conference presentation experience and multiple certifications.

EXPERIENCE

Cyber Security Researcher, Emerging Threats/Proofpoint - Missoula, MT Jun 2014 – current

Proofpoint acquired Emerging Threats in March 2015.

- Created 4000+ Suricata and Snort signatures to detect malware, exploitation, and suspicious behaviors.
- Created YARA signatures to detect various PE, Microsoft Office, Adobe Flash, Mach-O, and ELF malware.
- Trained and mentored staff on creating Suricata and Snort IDS signatures.
- Analyzed malware and threat data from internal and external sources, both proactively and in response to questions from customers.
- Conducted dynamic and static malware analysis on samples obtained from customer data and threat hunting activity in order to create detection signatures.
- Developed ad-hoc tools in Python to aid/streamline analysis of malicious network activity.

Cyber Security Consultant, LMG Security - Missoula, MT Feb 2014 - Apr 2014

- Conducted internal and external penetration testing and vulnerability assessments using Metasploit, Nessus, Nmap, Nexpose, and various scripts.
- Advised customers and provided reports detailing suggested improvements to IDS, incident response, and vulnerability management systems.

Security Engineer, Trace Systems Inc. - Afghanistan Apr 2013 - Dec 2013

- Re-engineered the network security boundaries of military bases in Afghanistan to convert key strategic network sites to more tactical firebases.
- Developed strategies to migrate user services to other bases and recertified networks.
- Surveyed closing US bases to create and execute a plan (EIP) to efficiently shut down communications.

Systems Subject Matter Expert, SAIC - Afghanistan July 2012 - Jan 2013

- Designed and implemented Snort IDS and analysis consoles for commercial wireless networks.
- Built and deployed authoritative DNS servers for the Afghanistan Ministry of Interior.
- Installed root DNS servers for coalition networks.
- Advised military leadership regarding project planning and execution across Afghanistan.
- Designed and implemented roadmaps to ensured projects complied with DoD regulations.
- Designed and deployed private cloud infrastructure.
- Implemented enterprise wide patching for servers.

Senior Security Operations Analyst, Quantum Research International - Kuwait Jan 2009 - July 2012

- Developed and deployed a robust IDS platform for the Regional Computer Emergency Response Team covering all DoD Southwest Asia networks (100+ Snort sensors) that included monitoring, alerting, statistical analysis of sensor interface, rule management, full packet logging and log rotation, SEIM/syslog integration, provisioning/configuration management, and security policy compliance.

Senior Security Operations Analyst, Quantum Research International (continued)

- Built log management systems to aid in correlation of security events. Monitored security information management tools (ArcSight) and performed incident handling and response for alerts.
- Developed threat hunting procedures to mine network data for anomalous traffic that indicated undetected threats and developed capability to retroactively search for discovered threats.
- Used data science tools to profile healthy network taps and developed techniques to identify/remediate unhealthy taps.

Senior Systems Engineer, Exelis/Harris - Kuwait City, Kuwait Feb 2007 - Jan 2009

- Engineered and deployed clustered Exchange supporting 6000 users.
- Administered enterprise systems servicing 45K users at 28 sites.
- Planned and executed Storage Area Network migration.
- Expanded and re-deployed legacy SAN as tiered backup storage.
- Expanded functional area of DoD Common Access Card Login.

Senior Systems Administrator, ITT Systems Division - Bagram Air Base, Afghanistan Dec 2005 - Jan 2007

- Led the 580th Direct Signal Support Team System Administrators responsible for the administration, troubleshooting and maintenance of Army classified and unclassified networks with 10K+ users.
- Planned and executed deployment of high availability Exchange cluster on an EMC SAN.
- Performed system backups, hardware/software installation, and upgrades.
- Conducted network vulnerability scanning and remediation.

Data Center Systems Engineer, WildTangent Inc. - Redmond, WA Aug 2001 - June 2003

- Planned, executed, and managed services in a datacenter supporting ~7M webdriver installations.
- Deployed IDS to monitor network security at the datacenter and corporate headquarters.
- Set up Active Directory infrastructure, disaster recovery, and developer support for corporate HQ.
- Executed policy and strategy to meet 99.999% uptime SLA.
- Set up web statistics reporting, web proxy, and server test lab.

Software Test Engineer, Microsoft - Redmond, WA Nov 1999 - June 2001

- Tested features and functionality on daily builds of the various Windows platforms.
- Improved and maintained test lab automation scripts used for installation and debugging.
- Performed ad-hoc kernel stress and fault injection testing.

COMMUNITY & LEADERSHIP

Member, Open Information Security Foundation (Oct 2018 - present) - Core team member/trainer responsible for conference presentations and contract work (documentation, scripts, testing). Co-presented at Suricon 2017.
CyberPatriot Mentor (Oct 2016 - May 2017) - Taught cyber ethics and defense skills to CyberPatriot (national youth cyber education) teams.

SKILLS

Malware Analysis, Python, Devops, Honeypots, IDS/IPS, Penetration Testing, Security Information and Event Management (SIEM). Threat Hunting

CERTIFICATIONS

CISSP #314055 • SANS GCIA Gold • MCSE (NT 4.0, 2000 Security, 2003 Security) • C|EH v6 • Security+