Grant Stavely

415-606-3947
grant@grantstavely.com

Summary

I love doing neat things with information systems and sharing that excitement with others through systems analysis, mentoring, consulting, and managing. I have a pragmatic and business driven security focus, and stress presentation, design, and usability. My current responsibilities are focused on information security engineering.

Skills

Incident response, forensics, Python, Perl, HTML, CSS, JavaScript, shell scripting, administration of GNU/Linux, FreeBSD, and Windows systems, IDS, netflow, syslog, log analysis, writing, and reporting

Professional Experience

Zynga, San Francisco, California **June 2010 – present**
Lead Security Engineer

Responsibilities:

- Evaluate security vendor technologies based on requirements to determine their effectiveness in Zynga's ecosystem
- Implement and own security vendor technologies that provide visibility into security issues inside the company (Vulnerability Scanners, Endpoint security, Intrusion Detection, Network Recording, Change Detection, Security Event Management)
- Perform discovery and vulnerability scans on networks and validate findings through penetration testing
- Validate perimeter and network security controls for effectiveness
- Perform configuration reviews on network devices and production systems and suggest potential remediation guidelines for any discovered issues.
- Develop and maintain automation frameworks to increase team efficiency
- Assist in technical investigation of security related events
- Produce technical and executive metric-based reports

Constellation Energy Group, Baltimore, Maryland **August 2006 – June 2010**
Security Analyst, Team Lead

Responsibilities:

- Led Fortune 120 information security engineering operations team of six analysts
- Directed threat analysis, network security monitoring (NSM), incident response (IR), vulnerability management, and host security control management activities
- Developed North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) based policies and procedures
- Designed and deployed network security monitoring solutions that integrate open source and commercial solutions to provide flow, full packet, and application protocol logging and alerting
- Created and deployed scripts enhancing network security monitoring capabilities in response to shifting threat tactics
- Designed tools for information security analysts to make analyst work repeatable, reportable, and standardized
- Designed and deployed tools and processes automating analysis of threat activity
- Tracked and reported security incidents, e-discovery cases, and forensic efforts
- Analyzed malware as part of incident response and host forensics efforts using commercial and open source tools
- Maintained diverse GNU/Linux systems and the services they provide
- Scripted in Python, Perl, and shell supporting all of the above responsibilities

Achievements:

- Graduated the Constellation Manager Development Professional (CMDP) course, a select program for prospective supervisors
- Attained SANS GIAC Certified Forensics Analyst (GCFA) certification
- Returned to night school to begin work towards the completion of a Bachelors of Science degree in Information Systems at the University of Maryland, Baltimore County (UMBC)
- Active in the information security community, attending ShmooCon, DefCon, DojoSec,

DojoCon, and multiple SANS and IANS events, as well as leading the Baltimore CitySec group, CharmSec

Outerbody Media, Columbia, Maryland **August 2004 – present**
System Administrator

Responsibilities:

- Maintain Exim, MySQL, Apache, and imapd virtual hosting services on FreeBSD and Fedora Linux systems
- Support Wordpress, TextPattern, and other small content management systems

Achievements:

- Migrated from local rack-space hosting to Amazon's Elastic Compute Cloud systems

Guru, Gaithersburg, MD **December 2001 – August 2006**
Senior Network Engineer, Team Lead

Responsibilities:

- Supervised nine consulting engineers who supported dozens of clients receiving both contract IT support and project oriented IT services
- Led technical engineering, sales engineering, product development, technology selection, training, and engineer mentoring
- Participated in weekly executive management meetings where operational, engineering, project management, sales, personnel, and client relations planning, direction and controlling decisions were made
- Provided IT support and systems integration for law firms, lobbyist organizations, non-profits, creative design, medical, dental, technology, biotechnology, and financial firms
- Led dozens of Microsoft Active Directory, Exchange, SQL Server, and Sharepoint implementations and migrations, Cisco PIX, Juniper Netscreen, and Watchguard firewall implementations, Symantec Antivirus, and Veritas BackupExec installations, and supported multiple line-of-business applications
- Administered both the public web site and company Intranet

Achievements:

- Developed and commercialized an SMTP spam and malware filtering solution using open source software and commodity hardware for my clients that could not afford third party mail filtering services

Education

University of Maryland, Baltimore County, Baltimore, Maryland

Bachelor of Science in Information Systems **Fall 2008 – June 2010**

- 130 credits attained

Bachelor of Arts in Imaging and Digital Arts **Fall 1999 – Spring 2001**

- 90 credits attained

Certifications & Affiliations

SANS GIAC Certified Forensics Analyst (GCFA) #3683 *Expires April 2012*
Member, FBI Infragard
Active U.S. Passport

Interests

CharmSec, Baltimore, MD **Spring 2008 – June 2010**

I helped lead a CitySec style meet-up and happy hour in Baltimore for information security professionals. In addition to scheduling CharmSec, I maintained the CharmSec twitter account, mailing list, and website.

Miscellaneous

I'm also interested in photography, graphic design, web design, home brewing, guitar, writing and rhetoric. Samples of my work can be found at http://grantstavely.com.

References *Available upon request.*