MICHALE N. EVANS

MBA / IM, CISSP, CCSP

MichaleEvans72@Gmail.com (253) 250-7039
http://www.linkedin.com/in/michaleevans *Twitter@michaleevans72*

PROFILE

A leader in information security for over twelve years, with a strong background that combines both business and technology. A diverse career history that began with serving on a Cyber Security Unit in the US military, then rapidly grew to include industries such as aviation, insurance, retail, government, and technology. Expertise in the areas of information security, penetration testing, incident management and response, and risk management. Extensive experience in leading and building high-performance teams.

Technical: Security Architecture and Design ▪ Penetration Testing ▪ Vulnerability Management ▪ Application Security ▪ Anti-Malware ▪ Mobile Security ▪ Mail Security ▪ Web Security ▪ Data Loss Prevention ▪ Next Generation Firewalls ▪ IDS/IPS ▪ SEM/SIEM ▪ Linux/UNIX

Management: Operations Management ▪ Strategic Planning ▪ Program Management ▪ Incident Response ▪ Governance ▪ Risk Management ▪ Compliance ▪ Business Continuity Planning ▪ Disaster Recovery ▪ Team Building and Leadership ▪ Process Improvement

PROFESSIONAL EXPERIENCE

Manager, Cisco Security Solutions

Cisco Systems 2013 – Present Seattle, WA

- Manage a national team of security consulting engineers, analysts, and solution architects in the delivery of security consulting services for Service Provider, Enterprise West and South, and smaller local market segments in the Western and Southern United States.
- Deliver an annual booking quota in excess of $20 Million in security consulting services.
- Handle resourcing, escalations, and delivery of security consulting services to over 100 active customers and projects led by 40-50 security consultants.
- Provided security consultation and expert guidance on Cisco's entire portfolio of security products and services to one of its largest $200+ million accounts.
- Architected, engineered, and implemented a global AAA solution for a top 10 tech giant that consisted of 20 Cisco ACS appliances and supported approximately 15,000 network devices.
- Collaborated with numerous partners, customers, and internal departments to conduct one of Cisco's first and largest ASA firewall / Sourcefire IPS integration efforts and beta tests.
- Managed and delivered a vulnerability management program that consisted of key elements of success such as a threat identification and classification matrix, priority-based auditing, and a cyclical remediation effort that protected all network devices for a global IT organization and resulted in an increased security posture.

Sr. Network Security Engineer

Alaska Airlines 2010 – 2013 Seattle, WA

- Design, implement, and maintain security infrastructure that includes: Cisco ASA Firewalls and VPNs, Checkpoint R75 Blade Firewalls, Juniper SA SSL VPNs, M86 Content Filters, Qualys Vulnerability Scanning, Symantec Endpoint Encryption, Tipping Point IPSs, Trend Micro Anti-Malware.
- Migrated existing Endpoint Encryption Solution to Symantec's PGP Whole Disk Encryption solution, enabling the business to expand their capabilities of key management and file-level encryption.
- Championed Alaska's second annual DLP discovery and remediation effort that inspected data at rest, data in transit, endpoint protection.
- Implemented Alaska's first Firewall Compliance, Auditing, and Security Life Management solution that improved performance, reduced the complexity, eliminated security loopholes, and greatly improved the security posture of the organization.
- Played a key role in Alaska's architectural design, vetting, and the implementation of its segregated Guest / Public Wireless network.
- Performed risk assessments and architectural designs for several Mobile Device Management (MDM) solutions that enable Alaska Airlines with such capabilities as security policy deployment and remote wipe capabilities for iOS, Android, and Window 7 Mobile devices.

Sr. Info Security Analyst

Pemco Insurance 2009 – 2010 Seattle, WA

- Led incident response through forensic analysis on systems and services by analyzing data, conducting investigations, addressing immediate risks, and reporting results to senior management.
- Performed regular risk assessments for PEMCO's critical business infrastructure and reported on the level of compliance in regards to company policies & standards that are based off of PCI-DSS, CIS, ISO 27002 (17799), GLBA, OWASP, and other industry standards.
- Mitigated vulnerabilities through configuration compliance audits and vulnerability assessments using scanning tools (CCM, IP360, Retina, etc.) to achieve and maintain good security posture.

Sr. Info Security Analyst, Consultant

Liberty Mutual / Safeco Insurance 2008 – 2009 Seattle, WA

- Administered 39 Blue Coat proxy and anti-virus servers for multiple states nationwide.
- Managed 73 Juniper firewalls and 20 Checkpoint firewalls supporting 45,000 employees worldwide.
- Reviewed and execute all requests related to the firewalls, proxy servers, and load balancers as the queue manager for the Threat Management team.
- Migrated Checkpoint firewall rule sets, as the lead firewall administrator, for 11 different field offices into a Juniper environment.

Lead Network Security Engineer

Smartronix 2006 – 2008 PSNS Bremerton, WA

- Administered and configured rules for dual load balanced Sidewinder firewalls that adhered to the Unclassified Trusted Network Protection (UTNP) policy.
- Utilized Cisco 7500 series routers to provide BGP/OSPF routing and to filter network communications, for the Pacific Northwest (PACNW) region that consists of Naval Bases: Bremerton, Bangor, Keyport, Whidbey, and Everett.
- Managed a split DNS suite of four Red Hat / BIND servers in accordance to the standards and regulations set by NETWARCOM.
- Delivered mail security for SMTP traffic with the use of multiple anti-virus/e-mail scanning servers running Symantec Mail Security.

Secure Communications Systems Specialist, AFSC - 3c051

United States Air Force 2002 – 2006 McChord AFB, WA

- Established real-time vulnerability management program to identify and prioritize critical vulnerabilities, non-compliance, malicious events, and blended threats.
- Restricted unauthorized access to network resources via Cisco and Sidewinder Firewalls.
- Managed, configured, and optimized 265+ Cisco routers and switches.
- Lead role in the design and implementation of a $500,000 wireless network for over 9,000 endpoints.
- Obtained a TS / SCI security clearance in order to handle classified government information.

EDUCATION

Masters of Business Administration, Information Management 2012

Aspen University

Bachelor of Science, Workforce Education and Development 2006

Southern Illinois University

Associates of Information Technology, Cum Laude 2004

Community College of the Air Force

PROFESSIONAL DEVELOPMENT

Certified Information Systems Security Professional (CISSP) *(311053)*
Cisco Certified Security Professional (CCSP) *(CSCO11104199)*
Cisco Certified Network Associate (CCNA)
SANS 660 - Advanced Penetration Testing, Exploits, and Ethical Hacking
SANS 560 - Network Penetration Testing and Ethical Hacking
SANS 507 - Auditing Networks, Perimeters & Systems
SANS 523 - Law of Data Security and Investigations

Lean Six Sigma (Green Belt)
ITIL Foundation Certification

Agora, Seattle Chapter
Infragard, Seattle Chapter
Domestic Abuse Women's Network (DAWN), Digital Literacy Volunteer