

MICHALE N. EVANS

MBA / IM, CISSP, PRIOR TS/SCI CLEARANCE

michaleevans72@gmail.com

<http://www.linkedin.com/in/michaleevans>

(253) 250-7039

[twitter@michaleevans72](https://twitter.com/michaleevans72)

PROFILE

A network and information technology leader for over fifteen years, with a strong background that combines both business and technology. A diverse career history that began with serving on a cybersecurity 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 ▪ Vulnerability Management ▪ Penetration Testing
▪ Network Security ▪ Application Security ▪ Anti-Malware ▪ Mail Security ▪ Web Security
▪ Next Generation Firewalls ▪ IDS/IPS ▪ SEM/SIEM ▪ Data Loss Prevention ▪ 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

Cybersecurity Leader, Consultant, and Owner

Cybersecurity Advisory Services, LLC Nov 2015 – Current Seattle, WA

- Drive the delivery of projects, policies, guidelines, and systems that increase efficiency and scalability.
- Consult with business leaders, architects, and engineers, providing guidance and expertise ranging from Managed Security Service (MSS) development to performing audits, risk assessments, and security needs evaluations on existing technology and security capabilities.
- Build and develop custom offerings ranging from Business Value Analysis (BVA) toolkits to Cybersecurity Framework (CSF) scorecards, templates and methodologies that all provide measurable and visible impact on security operations and tactical procedures.

Network Security Engineering Manager, Pacific Northwest Region

Check Point Software Technologies Apr 2015 – Nov 2015 Seattle, WA

- Managed a team of security practitioners responsible for delivering security engineering and architectural expertise for customers in the Pacific Northwest resulting in more than a 30% growth in annual sales revenues for FY2015.
- Orchestrated executive briefings between customer leadership and internal executives that focused on product roadmaps and design discussions, both providing strategic business value and an increased security posture.
- Led more than 20 customer and partner facing technology conferences and workshops, varying from global events such as VMWare Live and AWS re:Invent to local micro-segmentation boot-camps, evangelizing the growing sophistication of today's attacks and providing guidance through multi-layered defense strategies.

Regional Network Security Consulting Manager, Cisco Security Solutions

Cisco Systems

2013 – 2015

Seattle, WA

- Managed 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.
- Delivered an annual booking quota in excess of \$20 Million in security consulting services.
- Led resourcing, escalations, and delivery of security consulting services to over 100 active customers and projects led by 40-50 security consultants.
- 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.
- 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 supporting more than 15,000 network devices.

Sr. Info Security Engineer

Starbucks Corporation

2012 – 2012

Seattle, WA

- Lead engineer for Starbucks eDiscovery program, which included the implementation of Exterro's litigation management platform and a collection of Access Data's digital forensic solutions.
- Spearheaded a DLP deployment where a number of specialized systems and custom policies were utilized to detect and prevent the leakage of sensitive data both at rest and in motion.
- Managed risk by analyzing technology security threats and potential impacts to the business and helped define solutions to mitigate exposure by leveraging expert analytical and technical skills.

Sr. Network Security Engineer

Alaska Airlines

2010 – 2013

Seattle, WA

- Designed and implemented security infrastructure to include: 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.
- 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.
- 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 all major PACNW 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 e-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

- Two-time recipient of the 62nd Communications Squadron's Airman of the year award for exemplary service and expertise in Cyberwarfare.
- Established a 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.

EDUCATION AND PROFESSIONAL DEVELOPMENT

Masters of Business Administration, Information Management 2012

Aspen University

Bachelor of Science, Workforce Education and Development, Cum Laude 2006

Southern Illinois University

Associates of Information Technology 2004

Community College of the Air Force

Certified Information Systems Security Professional (CISSP) (311053)

Cisco Certified Security Professional (CCSP) (CSCO11104199)

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

Code Fellows Code 201/301 Software Development