Michael David Smith

Lead Technical Architect, Cyber Readiness and Response

Objective

To work in a positive team with people who are passionate about information security, and with this team contribute to the exploration of novel approaches to solve hard problems.

Education

B.S., School of Media Arts and Design, James Madison University (1999)
M.S., Computer Science with Information Security Concentration, James Madison University (2007)

Certifications

NSA CNSS NSTISSI No. 4011 (Certification for Information Systems Security Professionals)
NSA CNSS CNSSI No. 4014 (Certification for Information Systems Security Officers)
Project Management Professional (PMP)
Certified Information Systems Security Professional (CISSP)
Certified Information Security Manager (CISM)
GIAC Certified Penetration Tester (GPEN)
Certificate of Cloud Security Knowledge (CCSK)

Experience

Lead Technical Architect, Cyber Readiness and Response
Symantec — April 2012 – Present

I am currently responsible for the delivery, service definition, supporting research, and continuous process improvement efforts for all technical services offered by the Cyber Readiness and Response group, a part of the Security Business Practice, at Symantec. In this role as a technology leader I provide forward looking direction to ensure that our offerings are industry leading edge.

Senior Manger, Security Strategy and Advisory
Symantec — June 2002 – April 2012

I was responsible for designing, building, and operating a national security operation center for a large government client. This service extended to government clients in all 50 states. I assembled a team of security professionals that offer the following services via a 24x7 operational environment integrated with the Symantec Managed Security Services offering:

- Security Event Monitoring
- Incident Response and Computer Forensics
- Malware Analysis
- Network Vulnerability Assessment
- Web Application Vulnerability Assessment
- Security Advisory Creation

As part of my efforts to support this program I have led various technical projects including:

- Data mining security analyst performance information in order to drive efficiency and uniform security event analysis
- The design and implementation of a custom incident response and ticketing system
- MSS API development to allow the integration of Qualys Vulnerability Assessment data with the Symantec Managed Security Services offering
- MSS API development to facilitate the integration of our SOC database and ticketing system with the event, ticket and device data being fed to us from the Symantec MSS SOC.

Past Project Highlights

As a recognized technical and business leader at Symantec I have had the opportunity to participate in various strategic security offerings and initiatives. Examples of these are below:

Cyber Readiness Services Manager

I was selected to manage and drive improvement in the Security Advisory practice at Symantec. My role extended across all facets of this business including strategic direction, P&L management, team building, service creation and delivery, marketing and sales. I provided leadership to a national team of consultants focused on security research and project delivery.

Our portfolio of offerings included:

- Security Program Assessment
- Mobile Security Assessment
- Web Application Penetration Testing
- Mobile Application Penetration Testing
- Network Penetration Testing
- Product Penetration Testing

Symantec Global Security Practice Architecture and Product Management

I was selected to be the technical security architect for a massive outsourcing and global standardization project at Symantec. I was a member of a small M&A team evaluating various companies in Bangalore and New Delhi as part of a larger Symantec initiative to utilize shared delivery models between domestic and outsourced resources. At the time I was responsible for national P&L of Symantec Security Practice and as part of this effort I was asked to lead the coordination of globally delivered services with other national P&L leaders.

Symantec Joint Initiative with Accenture

I was selected to be the technical security architect and business process lead for a multi year multi million dollar Joint Initiative (JI) with Accenture. This effort included partnering with Accenture resources globally in order to develop Go To Market strategies, Offerings, and solution led designs for Data Loss Prevention (DLP) and Governance, Risk Management, and Compliance (GRC) solutions for large enterprise clients.

Principal Security Engineer
Riptech, Inc. July 2000 – June 2002

- Responsible for definition of baselines for all managed security products within the Riptech MSS offering, These baselines included the upgrade path for the device, configuration of the device, secure solutions for communication between the security operations center (SOC) and the device, as well as method of deployment for all managed devices.
- Coordinated with team managers to document and deliver this operational information to over 30 Riptech SOC engineers.
- Reported directly to the senior director of engineering on trends in the industry and how they affect the Riptech SOC and the security of Riptech SOC customers. Provided analysis of these trends to participate in Continuous Process Improvement (CPI) efforts.
- Designed solutions and managed implementation of enterprise level information security solutions for a number of domestic and international customers. Supervised 6 subordinates responsible for firewall and IDS integration into new and existing business networks. This includes the configuration of IDS, VPNs, secure mobile solutions and security policy definition on multiple firewall platforms (Checkpoint, Netscreen, PIX, Raptor, Watchguard).
- Supervised development of internal training materials and design of an intranet data warehouse for the engineering implementation division.

Security Consultant
Science Applications International Corporation (SAIC) December 1998 – July 2000

- Responsible for performing risk assessments, security test and evaluations, vulnerability assessment, penetration testing and formal certification and accreditation for selected government and commercial clients.
- Manager of the security lab environment for the information technology security division of SAIC. Duties as a Lab Manager included supervising one subordinate, network design and implementation, resource allocation, and equipment purchasing.