

# Martin G. Nystrom, CISSP

[martin@xianshield.org](mailto:martin@xianshield.org)

## Profile

Member of Technical Staff (MTS) for the Computer Security Incident Response Team (CSIRT) at Cisco Systems. Leads the global security monitoring team and provides guidance for incident response and security initiatives. Author and frequent conference speaker, provides briefings to customers via Cisco's Executive Briefing Program.

- Expertise in information security, particularly incident response, monitoring, application and database security
- Skilled in security consulting, auditing, policy-writing, and system hardening
- Experience guiding large projects toward secure implementations in a variety of languages and environments
- High-energy speaker, guest lecturer at several universities, conferences, executive briefings
- Highly-developed communication skills requiring the ability to rapidly understand business needs
- Productive in high stress and fast-paced environments, requiring skills in problem solving and coordination
- Business experience both e-commerce and biotech industries

## Experience

### **MEMBER OF TECHNICAL STAFF (MTS), CISCO SYSTEMS, RESEARCH TRIANGLE PARK, NC | 2002 - PRESENT**

Information Security Investigations Manager, CSIRT: Design and drive improvements to information security monitoring and incident response. Lead initiatives to improve preparedness and methods for responding to security breaches. Serve as escalation point for analyzing and resolving potential security breaches discovered by monitoring staff.

- Lead Global Monitoring Team, 15-person staff conducting 24x7 security monitoring of Cisco's network from multiple theatres. Developed scheduling and workload distribution to provide 24x7 monitoring. Formalized monitoring engagements and funding with clients. Drove improvements using Capability Maturity Model (CMM) for Services by improving quality assurance, engagement clarity
- Provided team for risk-based monitoring of extranet partners, new business units, and risky projects
- Conducted global threat summit with diverse IT staff, drove projects to mitigate identified threats
- Tested and drove improvements to Cisco products (CS-MARS, CS-IPS, others) by regularly engaging engineering/marketing based on deployment experience
- Developed standardized incident response handbook for global investigative staff, coordinated input and approval across HR, Legal, and internal auditors

- Co-authored book for O'Reilly Media based experience - *Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks*
- Delivered numerous briefings on security to Cisco customers and executives
- Deployed mobile rack-based solution for monitoring conferences and new business units. Rack contained network routers, switches, intrusion detection (NIDS) devices, and security analysis tools
- Lead team in building monitoring/response strategy based on threats to company
- Mentored security engineers on successful presentations to executives, conferences
- Led reorganization of CSIRT staff to provide 24x7 support, resilient tools, and approved incident response processes
- Led global deployment of NetFlow and event log collectors
- Lead investigations program to formalize engagement, response, and investigation procedures

Security Architect, InfoSec: Provided security direction for Cisco projects. Specializing in web security, consulted with IT project teams to provide secure architecture for large projects. Wrote policy and standards documents to address secure programming and deployment.

- Developed web auditing/remediation team to address web security vulnerabilities.
- Served as architect for web services security
- Developed database security strategy
- Delivered a series of "Nerd Lunch" presentations to security staff on database, web services, and web security
- Authored work for O'Reilly Media - *SQL Injection Defenses*
- Developed and delivered *Secure Web Programming in Java* course for global development staff
- Provided on-call incident response support: troubleshot high impact incidents, deployed firewall changes, investigated security incidents

### **IT ENGINEER, CISCO SYSTEMS, RESEARCH TRIANGLE PARK, NC | 2000 - 2002**

Lead Architect, E-Channels, Provided technical direction to team of engineers. Acted as consultant to business clients in exploring concepts for new applications. Provided architectural guidance to Sales IT Architecture Team. Sized and delivered tool enhancements and integration efforts. Develop and articulate technical vision. Mentored engineers through coaching, training, and guiding through technical challenges. Delivered series of presentations to e-commerce staff on internationalization, queuing, and b2b data exchange via XML.

Developed Partner Business Central - a portal into e-channels applications that allow Cisco partners to select, compare, and configure Cisco products, then interact with Cisco distributors for pricing, availability, and ordering. Product built in Java, using XML/XSL, CORBA, and Oracle, allows data exchange with business partners using XML over HTTP. Enabled RosettaNet integration for standardized message exchange with Cisco business partners.

### **SENIOR SYSTEMS ANALYST, SPHINX PHARMACEUTICALS, RESEARCH TRIANGLE PARK, NC, 1996 - 2000**

Application Developer, Architected, developed, and implemented distributed system for sample preparation, management, and distribution. Implemented development architecture; pioneered use of object technology for Sphinx. Hired and mentored staff in use of new development technique and language. Selected and implemented framework of reusable objects and patterns for software development, *saving over a year of development time*. Developed core object model and components for project teams. Implemented high-availability application infrastructure by deploying software to

multiple servers, scripting all deployments, and implementing SOPs. *New system reduced set plating time from 13 weeks to 5 days, and enabled preparation of 8 million samples in first year.*

Application Architect, Lilly Research Laboratories, Articulated guidelines, languages, tools for software development. Mentored developers in use of new technology (object-oriented design and programming). Selected contractors for projects. Established training plans for staff. Conducted proof-of-concept testing on various technologies (Java stored procedures, iPlanet, O/R frameworks, etc.). Helped developers launch projects by participating in first development cycles. Developed and published software development strategy for Lilly Research Laboratories worldwide. Delivered a series of global seminars on such topics as XML, Java & Oracle, Java with MQSeries, Java for web servers, getting started with Java, and EJBs. Architected, developed first phase of global compound registration system.

Developed and implemented *Linea* - a web-based spectroscopy data system. Built using Java and iterative development techniques. First version to production in only 60 days. System used for enhancing candidate lead optimization, stored over *20,000 spectra in just 4 months*.

#### **SYSTEMS ANALYST, ELI LILLY AND COMPANY, INDIANAPOLIS, IN, 1991 - 1996**

Developed system for global help desk and support. Created and deployed first client/server system using Remedy ARS toolkit on Sun Solaris servers with Oracle 6. Developed custom interfaces to e-mail and paging applications. Deployed global IT Service Management System (Remedy) to more than 800 users, enabled a unified support organization to provide centralized support for all 32,000 employees.

Administered InfoSys - a MVS/TSO based problem tracking application. Developed policies and procedures for enterprise-wide problem tracking and change management. Developed system to enable new enterprise-wide processes. Developed interface to electronic mail system. Integrated system with VM and electronic forms.

#### **CO-OP PROGRAMMER, IBM CORPORATION, CHARLOTTE, NC, 1990**

Wrote reports to allow senior management to measure compliance with workforce diversity goals. Used PL/I with DB2, tuned and refined program and database performance.

#### **CO-OP PROGRAMMER, IBM CORPORATION, POUGHKEEPSIE, NY, 1989**

Developed PL/I programs with IMS to control manufacturing of mainframe production lines.

### **Education**

**NORTH CAROLINA STATE UNIVERSITY** - Raleigh, NC

**Master of Engineering, Computer Science**

**IOWA STATE UNIVERSITY** - Ames, IA

**BA, Business Administration - Management Information Systems (M.I.S.) specialization**

### **Certifications**

**Certified Information Systems Security Professional (CISSP)**

*Specialization: Information Systems Security Architecture Professional (ISSAP)*

**Cisco Certified Network Associate (CCNA)**

## **Publications and Presentations**

[Security Monitoring: Proven Methods for Incident Detection on Enterprise Networks](#) (co-author)

O'Reilly Media, February 2009

[SQL Injection Defenses](#)

O'Reilly Media, March 2007

[Cisco Networkers](#), 2007, 2008, 2009

Inside the Perimeter: Six Steps to Improve Your Security Monitoring

[Forum for Incident Response Security Teams \(FIRST\) Annual Conference](#), 2007, 2009

Missing Clues: How to Prevent Critical Gaps in Your Security Monitoring

[OreDev Developer Conference](#), 2005

[Nine Ways to Hack a Java Web Application](#)

## **Referrals**

Available on request