Kenneth McGuinn

IT Security Architect contracted to DuPont

West Chester, PA - Email me on Indeed: indeed.com/r/Kenneth-McGuinn/e04f5e528390b0ed

WORK EXPERIENCE

IT Security Architect contracted to DuPont

Belcan - November 2013 to March 2016

• Design and implementation of security initiatives and managing those initiatives thru the project lifecycle
• Lead security architect for the FireMon initiative
• Contributing security architect for the Chemours spinoff
◦ Member of the review board to ensure that adequate security controls were being migrated from the DuPont to Chemours network
• Contributing security architect for the secure design of the DuPont Extranet
◦ Threat modeling.
• Contributing security architect for the review of Network Security Solutions and Security Technology Refresh
• Hosted meetings for stakeholders from the Global enterprise
• Refined and simplified the DuPont firewall change management processes by combining 2 disparate change management systems into 1
◦ Implemented FireMon Policy Planner
◦ Gathered workflow requirements from stakeholders, firewall owners and current workflow from existing tools to be integrated into a customized Policy Planner workflow
• Interaction with cross functional teams included telecom, audit, legal, infrastructure, security and change management
• Implemented Security Manager core module for approximately 500 Juniper and CheckPoint firewalls to report into FireMon
• Designed and integrated the approval process for access and authentication
• Dissemination of product functionality to security, audit, firewall owners, approvers and admin groups
◦ Creation of custom searches utilizing FMQL
◦ Implementing reports and recommending changes on shadowed and hidden rules, least and most used rules, unused rules etc. to increase performance and throughput of enterprise firewalls
◦ Path and traffic flow analysis
◦ Interpretation of firewall change requests into actionable firewall rules and determining what firewall change requests would need to applied
• Approver for firewall change requests on PCN (Process control network) firewalls.
• Reviewed and approved or denied firewall rule change requests by applying AP&C (Automation and Process Control) policy against requested rule changes
• CVI certified - Chemical-terrorism Vulnerability Information
• Researching security technologies and threats to determine if current controls are adequate
• Review of existing network design and the Juniper UAC architecture to ensure that the network is being vigorously defended against the current threat landscape
• Network Security Documentation
◦ Visio

Sr. Security Analyst

Automated Financial Systems - May 2012 to July 2013

• Management and administration of a QRadar SIEM

◦ Analysis of offenses and events
* Behavioral analysis of network flows
◦ Pruning false positives
◦ Flow analysis
◦ Custom rule and Building block design to trigger offenses and events
◦ Creation of searches in support of security incidents and investigations
◦ Generated reports for baselines and metrics
◦ Customization of dashboards and reports
• Active Directory
◦ Management of ADmanager Plus across 4 domains
* Bulk user creations, deletions, group modifications
* Report creation in support of audit
• Analysis of DLP (Proofpoint) logs
• Analysis of Checkpoint (Smartcenter) rules and logs
• SSL certificate management
• Nessus vulnerability scans
• Virus definition update audit
• Physical security

Consulting Senior IT Security Engineer

HCL America - October 2011 to March 2012

Successfully completed a short term contract in the role of a consultant with HCL America as a member of the governance risk and compliance team to complete a security gap analysis and vulnerability assessment

• Member of the Security Gap Assessment team
* Currently in the Plan stage of the ISO 4 phase model.
* Discovery of security gaps based on interviews and responses to questionnaires based on the ISO 27001:2005 framework
* Analysis of the client responses leading to a formal document which outlined the clients current security posture and the risks that would be assumed for non-compliancy
• Made the appropriate recommendations for the controls that would need to be put in place to reduce risk and be compliant
• Managing the vulnerability and network audit scanning project which culminated in scans of targeted servers in the global enterprise data centers
◦ Utilizing Nessus for the vulnerability scan and Nipper Studio for the network infrastructure audit
* Configuration of multiple scans on targeted servers across the enterprise
* Managing the scan from the perspective of asset identification, identifying the platform and application owners as well as giving guidance to the stakeholders on the results of the scan
* Creating the high level reports from the results for upper management
• Management and scheduling of resources across the global enterprise to bring the project to a successful conclusion.

Senior IT Security Engineer

MISI - February 2010 to May 2010

• Completed short term contract with MISI in which I was contracted to SunGard while a SunGard employee was on medical leave.
• Worked within the governance, risk and compliance sector of SunGard ITIL security model.
• Administration and log analysis for Websense data loss prevention
• Manage and administer the Rapid 7 Nexpose scanning

* Configure and initiate network scanning.
* Generate reports to track metrics of the scanning.
* Write procedural documents in support of the scanning process.
• Advise asset owners on security best practices and risk so as to comply with policy.
• Advise and work with auditors to ensure compliance.
• Advise and give guidance on how to implement best practices and meet control objectives.
• Member of the Archer Framework implementation team

Network Security Analyst

Jacob and Sundstrom - January 2009 to June 2009

contracted to the Department of Defense
• Primarily focused on the analysis of traffic crossing between military and non-military networks bound for military assets as well as military sourced traffic bound for non-military destinations.
* Identify non-compliant, malicious network traffic
* Identify real time external and internal attempts to exploit network and host based assets and applications via HTTP, SNMP, TCP/IP, FTP, IM etc.
* Relay appropriate information to mitigate threats to the firewall team
• Snort, TCPDUMP and a number of other proprietary tools are used in the analysis of both behavioral and Signature based rules.
* Write and recommend rules for implementation into the toolset
• Identify and report on assets containing malicious threat capability
• Contact with all levels of management for the remediation and knowledge sharing of events.
• Report tracking and management of remediation efforts.

TEKsystems - June 2008 to July 2008

• Engaged in a short term contract to design a solution for the remediation of network access vulnerabilities discovered during an audit
• Provide technical support to national account director during client meetings and follow up on any security centric issues the client requires to be addressed
• Coauthor the following statements of work with the account director
* Scope
* Project lifecycle details
* deliverables
• Designed a Tacacs+ solution for Network Access Compliance
• Engage with client technical staff for all pre solution implementation discovery

Security Vulnerability Manager for the Cingular Wireless NE

Cingular Wireless / AT&T Mobile - August 2005 to December 2007

region
• As an original member of the vulnerability management security initiative for the NE region I implemented processes and procedures to get the initiative off the ground and to review, refine and implement these procedures and processes when applicable
• Introduced Preventsys as a remediation and automated work flow management tool along with managing the project lifecycle.
• Conducted product evaluations of security tools in support of the following security initiatives
◦ Vulnerability scanners
◦ IPS AND IDS
◦ Security management toolsets
◦ Workflow management

◦ SIEM
• Generated risk assessment documentation for variances
• Managed the remediation and mitigation of vulnerabilities for all core network platforms (OSS, SGSN, BSC, RNC, MSC, HLR, and VLR) in all markets of the Cingular Wireless Northeast region for Windows, UNIX and Solaris platforms.
• Vulnerability Scanning
◦ Nessus, nCircle, Retina
• Correlation and workflow tools (Preventsys)
• Initiated policy and procedures for hardening of UNIX and Windows based servers)
• Team member for SOX compliance and audit remediation
• Team member to assess ISO 17799 controls.
• Administer the archiving of all security related requests and correspondence in support of due diligence.
• Represented the NE region on security panels for a variety of security initiatives.
• Access Management
• AD and Unix
• Account builds
• Account scrubs
• Audit of role based permissions and management of access control matrix
• Wrote policy and the procedures in support of policy as well as the review of existing policy to ensure that they were current.
• Worked with all the market operations managers to disseminate security policy, procedures and processes.
• Working with the platform owners I resolved any issues that arose due to remediation requests on the respective platforms that they own.
• Acted as a security ambassador to instill the need for security and the timely remediation of vulnerabilities.

IT Security Engineer

Tek Systems - July 2004 to January 2005

• Project manager and Team Lead for the Bristol-Myers Squibb Desktop Firewall Initiative
* Managed the project from inception thru test pilot.
* Authored all project documentation.
• MS Project document
• Firewall summary and recommendation documents
• Firewall criteria
• Project charter, scope, stakeholder, test plans etc.
* Conducted the assessment of the current firewall technology and based upon those findings made recommendations for the initial vendor selection.
* Developed criteria for 2'nd round of vendor selection.
* Developed test strategy for test phase and conducted the actual testing.
* Developed the strategy for firewall components that would be implemented.
* Developed strategy, scope and objectives for pilot phase.
* Set up and evaluated McAfee, ISS, Sygate and Zone Labs firewalls along with the enterprise management components.
* Created line item criteria to be used in the vendor reverse auctions
• This resulted in significant price reductions from initial vendor quotes.
* Created objectives that vendors would be tasked with.
* Reviewed Vendor Statements of Work for accuracy.
* Actively participated in and contributed to the BMS security focus group.
* Headed project team meetings and created applicable PowerPoint presentations.
* Gave presentations focused on various aspects of security to the global BMS security group.

IT Security Engineer

Wyeth - March 2003 to March 2004

Security analysis for a 50,000 node network
Administered an ISS Black ICE firewall
Implemented a ISS Black ICE Pilot
Vulnerability scanning - Nessus and Retina.

Desktop and Network Infrastructure - June 1981 to March 2003

design, service and support

EDUCATION

Electronics Technology

Denver Institute of Technology - Denver, CO
March 1980 to April 1981

Liberal Arts

Penn State University - Lima, PA
September 1974 to June 1975