Sept 25, 2024

Michael B Evans

Human Resources Office:

I am applying for the position of Chief Information Officer, and Associate Vice President. Not only have I been in education for over 20 years as an administrator, Information Technology, Information Security and adjunct professor, I have been the CIO/CISO/IT Director for over a decade. For more than 30 years, I have securing, managing/building networks, managing data centers, monitoring systems, Information Security, Cisco Routing/Switches/Firewalls, Palo Alto firewalls, and performing compliance/risk/governance. Not only do I have a CISSP, years of experience securing infrastructures, 24x7x365 day operations, privacy, monitoring, governance controls, and compliance but have experience leading teams/budgeting in the field of Education. I am also currently an adjunct professor at Syracuse University.

Currently as the Info Security Analyst Senior at USAA, I am completely remote and am responsible for the Cyber Threat Operations Center compliance/governance over the past year. I have knowledge and expertise in all the various information security frameworks. For USAA I've been doing every form of compliance, PCI-DSS, federal, banking, risk, model risk, controls, etc. that involves the CTOC (Cyber Threat Operations Center), Red Team, Detections Team and Infrastructure teams.

At NYSERNet, I directed Information Technology, Communications and Information Security but I have also developed a Vulnerability Management software program for purchase by the higher education institutions in NYS. I have also implemented redundant server data centers in Syracuse/New York City including VMHosts, Palo Alto firewalls, VPNs, internet connections, and backups—just to name a few things. Being NYSERNet's first security officer, I wrote the first security policies, business impact assessment, risk assessment, disaster plans and implemented MFA, device logging, SIEM, disaster recovery, and risk management processes.

As the IT Security Manager/CISO/IT Manager at DUMAC, I started this position with no security controls, no SIEMs, monitoring, no security policies and procedures. A year and half later at DUMAC, I had them PCI compliant for the second year in a row. The first year, it took 2 months of clean up to pass compliance. The second year, our assessor left 2 days early and there was no cleanup necessary. I also provide PCI-DSS compliance, vulnerability/assets scan, and forensic investigation services to many Wendy's, Churches, Popeye's, Speedways and grocery stores throughout North and South America. I've done data classifications, risk assessments, vulnerability scans, log correlations, and implemented NIST/SANS compensating controls. I've also worked with the installation teams to lock down Windows and Linux images according to NIST and CIS and implemented HIDS using OSSEC.

Examples of key achievements include:

- Build Cisco routing/switches Layer 2/3 for each business for I've worked in for the past 30 years.
- Implemented firewalls in production for NYSERNet, DUMAC and Colgate for both Palo Alto and Cisco firewalls.
- Successfully implemented service provider security practices, policies and procedures to pass PCI-DSS compliance August 2016, and June 2017
- Provided assistance, direction and guidance with more than 100 Wendy's, Church's Chicken, and Speedway to help them pass their PCI-DSS compliance
- Successfully turned around an under-performing technology teams through mentoring, training and development, strong performance management and goal setting.
- Built, designed and implemented a Security Operations Center to identify global incidents more quickly and geo-locate successful authentications to limit exposure.
- Implemented a first of its kind central monitoring function for all key systems, designed to identify and resolve issues before they affect business operations at both NYSERNet and DUMAC.

From September 2015-December 2017, I completed my online Master of Information Assurance with a concentration in Cyber Security including classes in Computer Forensics, Network Forensics and Malware Analysis and Response. Not only do I have the classroom work, but I have also been involved in many breaches including Wendy's loss of millions of credit card numbers where I've had to use my forensics skills. I have a huge advantage over many other individuals in forensics with broad background and experience in software, networking, systems and certifications including ISO/2700x, HIPAA, PCI-DSS, PA-DSS, NIST and SANS.

Please review the enclosed resume and feel free to contact me at your earliest convenience. Thank you in advance for your consideration and I look forward to your call.

Sincerely,

Michael B Evans

Michael B Evans

MICHAEL B EVANS

OBJECTIVE

Attain a position allowing me to show my extensive experience in IT/InfoSec Management, security, networks, servers, enterprise management, mentoring employees, project management and development in enterprise networking solutions and systems in and around the data center in risk, compliance and governance.

WORK EXPERIENCE

Info Security Analyst Senior Apr 2022 – present
USAA, Remote

Job Responsibilities: Complete compliance for the Cyber Threat Operations Center including Enterprise Risk Management, Enterprise Model Risk Management, Control Testing and attestation; NIST, CyberSecurity Risk Indicators, Auditing and Risk Compliance, PCI, Risk Management Framework, Key Risk Indicators (KRI's), Key Performance Indicators (KPI's). AttackIQ purple teaming using the Mitre Att&ck framework. Cloud Review Panel processes, Business Application Risk Reviews. Review custom Cyber Detections using ELK. Building Custom Threat Detections and testing with AttackIQ; Red Team Operations.

Adjunct Faculty Member Jan 2022 – present
Syracuse University, Syracuse, New York

Job Responsibilities: Teach IST452 Advanced Networking (Cisco CCNA certification class)

Director of IT / Information Security Officer Jan 2018 – Apr 2022
NYSERNet, Syracuse, New York

Job Responsibilities: Manage the Information Technology, multiple Data Centers, compliance and build security services for Colleges and Universities; Budgeting; IT Staffing; Software Development; Risk Management and Planning; Vendor Management; Security Architecture planning. Hardware/Firmware upgrades. Firewall/IPS/IDS monitoring and configuring. Implementing/Testing DR, BCP IRP plans. Creating standard policies for Security Devices; Evaluate/POC new Security Services and Technologies for ISP, University, College use; Hardening Security device configurations; Vulnerability scans; Pen Testing; Patch Network/Server devices; Security Management: Write and modify security policies as necessary; Proactively monitor the environment for patch compliance, vulnerabilities and other threats; File Integrity Monitory; Traffic analysis through Firewall, IPS/IDS; Understand critical business services delivered from IT Operations and ensure they are compliance and secure; Design, build and implementation of IT Security Architecture. Experience providing detailed plans and managing the resolution of highly complex issues and problems Analysis; Perform yearly NIST Risk Assessments; Stay current with possible threats. Working knowledge of SANS, NIST and CIS frameworks including 800-30, 800-171, Cybersecurity Framework 1.x.

Accomplishments: Built and implemented NYSERNet's multi-city Syr/NYC VMWare clusters, Active-Active Palo Alto firewalls, multi-city LAN and centralized authentication for no downtime. Implemented NYSERNet's first logging, Data Loss Prevention (DLP), security policies, Risk Assessments/Risk Management, Vulnerability Scanning, ELK SIEM, disaster recovery (DR) plans, off-site and off-line backups, business continuity plan (BCP). If they choose to NYSERNet could now pass a SOC audit.

CISO/IT Security Manager April 2016 – Jan 2018
DUMAC Business Systems, East Syracuse, New York

Job Responsibilities: Manage Network and Software Development staff; Budgeting; Vendor Management; PCI-DSS Compliance; Qualified Integrator and Reseller (QIR) Compliance; Security Architecture planning. Hardware/Firmware upgrades. Firewall/IPS/IDS monitoring and configuring. Implementing/Testing DR, BCP IRP plans. Creating standard policies for Security Devices Evaluate/POC new Security Technologies Hardening Security device configurations;

Vulnerability scans; Pen Testing; Work with Network/Server Teams to ensure patches and packages installation; Security Management: Write and modify security policies as necessary; Proactively monitor the environment for patch compliance, vulnerabilities and other threats; File Integrity Monitory; Traffic analysis through Firewall, IPS/IDS; Understand critical business services delivered from IT Operations and ensure they are compliance and secure; Design, build and implementation of IT Security Architecture. Experience providing detailed plans and managing the resolution of highly complex issues and problems Analysis; Perform yearly NIST Risk Assessments; Work with Application Development Teams to ensure privacy of PII and other sensitive data; Stay current with possible threats. Working knowledge of SANS, NIST and CIS. Currently exploring SOX 2 and ISO 27002 compliance.

Accomplishments: Designed and built Security Operations Center locating all employees, customers and potential attack interfaces for 5 remote locations (Houston, Oklahoma City, Indianapolis, Fort Worth, New Hampshire) and over 150 remote employees covering 11 time-zones and 2 continents. Geolocation of IP addresses to track successful logins of employees and customers into all secured servers. Completed business first PCI-DSS compliance 2016-17, 2017-18; Qualified Integrator and Reseller (QIR) trainer (over 30 employees successfully passed—zero before I built the training program). 2,106 qualified installations since February 1.

Interim IT Director/CISO/IT Security Manager March 2017 – Oct 2017
DUMAC Business Systems, East Syracuse, New York

Job Responsibilities: Ensure the business systems, technical framework, and all software applications used by the business units operates with minimal unscheduled downtime, ensure the corporate systems are strategically aligned and maintained with the corporation's goals and direction, responsible all aspects of data security, strategic and capacity planning, disaster recovery processes and procedures, manage vendor relations and relative outsourcing arrangements, monitors budget/capital items related to software & hardware, manage assigned staff regarding salary, promotion/demotion, mentoring and hiring/firing

Accomplishments: Established first hardware/software refresh budget viewing +/- 10 year windows. Implemented secure VLANs, Golden Image Servers, Implementing Hyper-Converged Environment for Active/Active Data Center Redundancy

Senior Network and Systems Analyst/Acting CISO Sep 2014-April 2016
Colgate University, Hamilton, New York

Job Responsibilities: Scan server and client VLANs for vulnerabilities, determine if the vulnerability applies to the systems and patch accordingly. Monitor event logs and assets in SIEM to determine if systems are under attack. Packet capture as necessary and use network forensics skills to determine if the attacks are real. Write and update security policies and procedures are necessary. Implement PCI compliance, and follow FERPA data requirements.

Accomplishments: Start of PCI compliance, built secure NYS Health Care Research servers for Geo tagging medical issues to see if there is a correlation, built Asset Inventory and Data Classification across the University, vulnerability scanned all staff client machines and servers to determine risks. Worked with server owners to mitigate, recast or accept risk.

Systems include Tenable Security Center, Nessus, QRadar, Wireshark, and other security tools

Senior Network and Systems Analyst May 2006 – April 2016
Colgate University, Hamilton, New York

Job Responsibilities: Build, design, maintain, secure, support and budget wired and wireless networks, redundant ISPs, redundant data centers, generators, battery backups, system backups and firewalls so the University has "no" downtime. Analyze and resolve network/server issues. Build project plans using MS Project. Documentation of network and services using Visio.

Systems include Cisco 1002/9001 routers, Cisco Catalyst 65xx//68xx, Multi-context Cisco blade firewalls, Active-Passive Palo Alto 5585/5002 firewalls, 500+ Cisco switches, 150+ VLANs, HP 3Par, HP EVA4400, HP StorageWorks, HP MSAs,

HP Insight, 1000+ Aruba APs, 3 Aruba Controllers, 16 VMWare hosts, 150+ VMs running Windows 2012r2-2008r2/Red Hat Linux, 4 Clustered SQL Servers, 9 SQL Servers (2005-2012), multiple Microsoft Active Directory domains, DHCP, VPN, DNS, NTP, NAT, Exchange, MS Project, Visio, MS Word, Excel, Access, Interfaces into Oracle, BGP, OSPF, Powershell,VMWare 5.5, VDP, NetPhysics (OPTnet), NetDirector, Wireshark, SolarWinds Engineers Edition

Accomplishments: Virtualized entire physical datacenter with minimal downtime. Designed, and implemented active-active redundant ISPs, Routers, Firewalls and fiber to active-active datacenters. Part of team that designed, built, and maintained new Aruba wireless system. Designed, built, upgraded and maintained our Microsoft AD domains, internal/external/private DNS, DHCP, VPNs, and SQL Clusters. Worked with vendors to put in new single mode fiber to the 189 building and closets. Implemented redundant linked port-channels for all the buildings. Designed and implemented the VLAN plan for Cisco phones, environmental controls, fire alarms, one card devices, servers, VMWare blade center and all wired/wireless client devices.

Director of Web Development Jun 2002 - May 2006
Colgate University, Hamilton, New York

Lead team that built in-house portal and dynamic home page using ASP.NET and SQL. Presented project at 3 National conferences. Managed Microsoft onsite/offsite Web server farms. Worked with Network group managing routing and firewall installation and day-to-day operations. Built updates into Active Directory database from administrative Oracle systems to increase efficiency.

Web Master Sep 1998 - Jun 2002
Colgate University, Hamilton, New York

Managed web servers, built new public website, coordinated updates and site renovations with 68 departments/offices, built scripts for dynamic updates of campus directory, calendaring, and AD user and group creation

President/Owner Jan 1994 - Sep 1998
Business Visions, Syracuse, NY

Network, Systems, and Web Development Consultant throughout the NY, MA, CT, and PA

New Product Development Manager Jan 1992 - Dec 1993
The Cbord Group Inc, Ithaca, New York

Developed, designed and programed C++ application ordering and inventory system to sell to all the thousands of customers of the 50+ Sysco Food companies. Also built interfaces into their various business systems.

MIS Manager Mar 1990 - Dec 1991
Business Records, Syracuse, New York

Managed 16 customer support personnel (local and remote) which supported the 250+ counties in various east coast states, designed, implemented and coordinated equipment/personnel arrivals for a customer upgrade program, held impromptu customer feedback meetings

Academic Dean Sep 1987 - Dec 1989
Bryant and Stratton, Syracuse, NY

Transferred back to Syracuse to help convert the students and faculty to the new curriculum

Academic Dean Sep 1986 - Sep 1987
Bryant and Stratton, Albany, NY

Part of a 3 person team that converted Albany Business College to a Bryant and Stratton. Built schedules and budget/cost models in Excel for all the students and faculty to determine cost benefit analysis for best transition

Computer Instructor Jun 1985 - Dec 1997
Bryant and Stratton, Syracuse, NY
Taught day/evening computer programming and systems classes

EDUCATION
Bachelor's Degree, Computer & Information Sciences, Syracuse University | Syracuse, New York
Master's Degree, Information Assurance with Cyber Security, Regis University | Denver, CO
Master's Degree (expected 2026), Data Science, Regis University | Denver, CO

CERTIFICATIONS
CISSP, CCNA, QIR, Security+, MCSE
CISM (taking exam Oct 2024)

SKILLS
Python, Pandas, ELK, AlienVault, MaaS 360, Tenable Security Center, Nessus, QRadar, Metasploit, OSSEC; VMWare ESX, VCenter, and VDP; Wireless rogue detection; I3 Camera Systems; NetAXS Honeywell Security Systems; BitDefender, Comodo, Semantic EndPoint Protection, Cisco switches, ASR routers and firewalls, MS Windows Server 2012, 2008 R2, 2003, 2000, NT, Microsoft SQL, Active Directory, DNS (Dynamic), DHCP, Exchange, IIS, VPN, NLB, Clustering, Powershell and VBScript; HP DL series servers, blade servers, MSA and EVA Storage; Allot Bandwidth Shapers; Barracuda, Cisco, Ubiquity and Aruba Enterprise Wireless; APC UPS's; LogMeIn; NCR Command Center; SolarWinds; SANS; NIST; CIS;
POS systems (Aloha, Xpient/IRIS, Maitre'd, Digital Dining, Connected Payments), Visual Studio,C#,Powershell

COMMUNITY
Baseball, Soccer and Basketball Coach 2004-2017
Canastota JV Baseball Coach 2013-2018
Canastota Modified Soccer Coach 2014-2017
CubMaster 2006-2013