Ryan W. Voloch, *CISSP, GCIH*

Pittsburgh, PA
Email: LinkedIn@voloch.com

EDUCATION

R.I.T. - Rochester Institute of Technology, Rochester, NY
Bachelors of Science Degree in Information Technology, *Honors*
Networking & System Administration Concentrations
Professional GPA: 3.8

SKILLS

- IT Technical Engineer and Project Manager for the successful implementation of over ten major enterprise security solutions.
- Extensive security, network, and system administration experience.

Network Engineering
Advanced TCP/IP Understanding
Network Statistic /Monitoring Systems Cisco IOS PIX, ASA, previous CCNA
Backbone Routing, VPN & Connections

System Administration
Network Administration Unix & Win: AD, DNS, DHCP, SNMP & Mail servers
UNIX: NIS, NFS, FTP, HTTP & Samba, user management
UNIX/Windows Hardening & Auditing
VMWare

Enterprise Security Systems & Tools
SIEM: ArcSight, RSA Envision
Integrity: Tripwire Enterprise
DLP: Vontu, OpenDLP
Scanners: Nessus, Qualys, Nexpose, Burpsuite Pro, Acunetix
IPS/IDS: SourceFire/Snort,ISS
Pentest: Backtrack toolset, metasploit
WAF: TrustWave WebDefend
AV: SEP, SCEP/SCCM, TrendMicro

Risk Management
Modulo, Allgress

Programming & Scripting
bash, perl, python, PHP, SQL,VB, BASIC, Pascal, C++

WORK EXPERIENCE

Education Management Corporation (EDMC), Pittsburgh, PA
Security Analyst III *(November 2011 – Present)*
Security Analyst II (April 2011 - November 2011)
Security Analyst I (January 2009 - April 2011)

- Security Information Event Management SIEM: Matured SIEM by designing and implementing use cases to replace the third party provided managed security service provider, resulting in cost savings, increased visibility, operational efficiency and accuracy; Implemented Automated Shunning Framework, blacklist integration, and log feed health monitoring; Integrated IP management system with network asset model to support prioritization and efficient routing of alerts; Implemented over a dozen different connectors, including custom connectors; Developed and managed a use case queue for prioritizing, initiating and tracking the SDLC of SIEM use cases; Identified business requirements, evaluated multiple SIEM solutions, performed RFP and fully implemented SIEMs; Directed and supported a team of System Administrators that managed connectors.
- Security Incident Response: Developed, maintained and matured Security Incident Response, policy enforcement technologies, metrics, processes and procedures; Acted as Security Response lead incident handler.
- Data Loss Prevention: Implemented file quarantining for company shared network drives and detection on company intranet; Performed system upgrades and matured detection policies; Implemented blocking outbound emails with PII; Developed and maintained DLP Security Operations procedures.

- Risk Management: Designed future state processes and requirements for maturing the Risk Management program to increase efficiency, accuracy, and timeliness of results to business owners; Performed proof of concepts for Modulo and Allgress Risk Management systems; Served as Data Custodian of the Risk Management database and matured it by implementing changes to increase reporting accuracy and analyst efficiency; Trained and guided team members to handle data custodian duties.
- Vulnerability Management: Assisted with procurement of an in-house vulnerability scanner that replaced a managed service, resulting in cost savings and increased visibility; Developed and coordinated PCI ASV scans; Managed the vulnerability scanner and ensured critical results are sent to the Risk Management program.
- Security Assessments: Performed more than 80 Security Assessments for schools, SAAS vendors and new systems which resulted in identifying, assisting and resolving security and continuity risks to the business. Assessments included local configuration reviews, IT and business interviews, and web application testing; Developed and executed a repeatable vulnerability assessment program for schools and corporate services.
- Security Operations: Developed and implemented a replacement Security Operation analyst checklist framework and procedures, resulting in a significant amount of decreased operational resource hours; Managed the third party managed security service provider for firewall and IDS monitoring; Matured the service by implementing processes to respond to monitoring system issues using in-house operations staff; Performed Security Operations checklists as part of team rotation; Assisted in the development and delivery of security awareness training programs.
- Security Engineer/IT Project Management: Acted as security consultant and IT Project Manager for the implementation of Endpoint Protection system. As a result, proper configuration and processes were in place to increase workstation integrity; Identified business requirements, evaluated Endpoint Security/Antivirus vendor solutions and consulted the implementation team; Performed system hardening and developed operational controls for a point-of-sale system that exceed PCI compliance; Assisted with Hard Drive Encryption project.

Giant Eagle Supermarkets, Pittsburgh, PA

Data Security Analyst (August 2003 - January 2009)
Network Services Intern (Summer 2001 & 2002, Winter 2003)

- Fully researched, purchased, and acted as project manager for the implementation of multiple enterprise security systems such as SIEM, Network Access Control, Intrusion Prevention, business-to-business PGP file transfer service and email encryption.
- Assisted with third-party PCI, HIPAA, and Sarbanes Oxley security audits and assisted IT teams with remediation efforts. Was highly involved in the process of attaining Level 1 PCI compliance.
- Developed Data Classification framework, Incident Response procedure, Data Security Policies, Network Security Strategy, emergency/root ID sign-out process and Security Awareness program.
- Managed multiple access control infrastructures and processes to ensure proper access is given to users.
- Supported 24 hour Help Center and Computer Operations Center.
- Assisted the Network Engineer and responsible for WAN, LAN and wireless network troubleshooting.
- Assisted with design and implementation of 802.11b to 6 warehouses and 210+ store locations.

OTHER ACTIVITIES

- Growth group leader for Impact Christian Church
- ISSA member and regular attendee
- Second vice president of the Kappa Delta Rho Fraternity at R.I.T., 2003
- Community Service, Philanthropy Chair – Raised +$2,200 for Red Cross
- Supervisor for RIT's Network and System Administration Labs, 2000-2003
- Senior participant of R.I.T.'s Connections Technology Lab
- Captain of 40 member men's rowing team, 1999