Matt Pogue

Technology Expert and Hacker Extraordinaire

p: (314) 500-3194
e: matt@mattpogue.com
Lake St. Louis, MO 63367

Career Summary

A senior IT specialist with over 25 years of experience in all aspects of enterprise IT, and a hacker in the truest sense of the word, Matt brings to the table a depth of knowledge and a passion for problem solving that sets him a cut above his peers in the industry.

Some of the highlights of Matt's career experience include:

- Preparing a Fortune 500 enterprise for SOC2 certification and developing system automation using Ansible, Python, and shell scripting.
- Designing, implementing, and maintaining enterprise security systems, including both network- and host-based intrusion detection and intrusion prevention systems, firewalls, centralized logging platforms such as Splunk and McAfee ESM, and endpoint security packages including McAfee ENS and Symantec Endpoint Protection, among others. This includes re-architecting existing systems in order to improve performance, increase visibility, and improve overall accuracy.
- Assist with ISO certification process – ISO 9001 and ISO 27001.
- Designing, implementing, and maintaining secure network environments using multiple firewall architectures – primarily Cisco ASA, Checkpoint, Linux IPTables-based, and FreeBSD pf-based.
- Administering and maintaining Active Directory and Microsoft Exchange environments for companies of all sizes – from small one-site organizations to global corporations with 5,000+ employees and a global presence.
- Designing, implementing, and maintaining virtualization environments using multiple technologies, including VMWare, Microsoft Hyper-V, Linux Qemu/KVM virtual machines, and Linux (LXC) and Docker containers.
- Performing DevOps tasks, including standardizing server builds, implementing server configuration management, automating server updates, and integrating security auditing and vulnerability management with ServiceNow.
- Performing numerous computer forensic investigations, while working in conjunction with internal corporate legal departments, to ensure proper data collection, chain of custody, and adherence to established procedures. By ensuring that all relevant laws and corporate policies/procedures were followed, the team's findings were admissible in court and able to withstand the scrutiny of cross-examination in those instances when criminal charges were pursued by the corporation or other legal entity.
- Developing an enterprise-wide Vulnerability and Threat Management Program, including guidelines that became official corporate threat management policy. In addition, evaluating, comparing, reviewing, and procuring hardware and software. Developing procedural guidelines for penetration testing and vulnerability assessment in conjunction with multiple teams and internal resources from the legal department.
- Architecting, implementing, and administering enterprise-class security and information event management (SIEM) solutions. After successful SIEM deployment, developing and maintaining event correlation logic, delivering actionable intelligence to systems administrators and security analysts within the organization.

Systems Director
Worldwide Freight Management
February 2019 - Present

- Responsible for all aspects of IT within the organization, including budget development, purchasing, information security and auditing, and operations.
- Continuing development on Production project management application, Microsoft .Net Core technology stack, including migration of legacy .Net Framework code.
- Develop multiple customer-facing APIs to provide EDI integration with customer purchasing systems.
- Administer and maintain on-premises Active Directory environment including Azure AD/Office 365 synchronization, security auditing and policy management, account management, and application and mailbox management.
- Develop standardized builds for both servers and workstations, implement server configuration management with Ansible.
- Deploy new pfSense firewall platform to all locations and build and configure VPN tunnels and VPN client access. Migrate OpenVPN tunnels to WireGuard.
- Develop and maintain an automated process to install server updates.
- Deploy the Zabbix system monitoring application to monitor all servers and network hardware.

Senior Automation Engineer (Contract)
Express Scripts
May 2018 – February 2019

- As a member of the SOC2 Engineering Team, perform tasks related to enterprise-wide preparation for SOC2 certification on approximately 6,000 Linux servers and 12,000 Windows servers.
- Work with members of the Unix Engineering team on the ongoing deployment of Ansible for configuration management, including migrating systems from both Puppet and Chef to Ansible Automation Platform (at the time known as Ansible Tower).
- Develop Python and shell scripts to automate user account management tasks based on inputs provided from the SOC2 administration team.
- Develop a Python-based web application using the Django framework to track team automation tasks, including user account maintenance, affected servers, and scheduled changes.
- Work with the enterprise server build team to integrate SOC2-related changes to the automated build process on RHEL 7.
- Assist in transitioning the server build process from an RPM-based process to Ansible.
- Work with other members of the SOC2 Engineering Team to develop Ansible scripts to automate various SOC2-related tasks, including user management and patch management.
- Work with members of the Unix Engineering team to develop and deploy patches across all Unix servers in the enterprise, including RHEL 5, 6, and 7, HP-UX (multiple versions), and AIX (multiple versions).
- Develop and deploy multiple Production changes after first deploying to both the Development and Staging environments.

Information Security Analyst (Contract)
Ascension Healthcare
October 2017 – April 2018

- Perform tasks related to the enterprise-wide deployment of McAfee Enterprise Security (ENS) to approximately 175,000 endpoints, including servers (multiple Windows versions, Unix, Linux, and AIX), workstations, laptops, tablets, mobile devices, and specialty hardware such as storage controllers. Most of these devices are being upgraded from McAfee Virus Scan Enterprise (VSE).

- Develop multiple enterprise processes, including:
    - A process for internal application developers to obtain a trusted internal certificate for code signing, then using the certificate to sign internally distributed applications. The code signing certificates are used to ensure the application's trust level within the McAfee Global Threat Intelligence (GTI) database.
    - A process for testing versions of McAfee ENS upon release.
    - A process for testing enterprise application compatibility with ENS.
- Develop content and present multiple "Tech Talk" sessions to the Endpoint Protection Team. These talks covered the subjects:
    - Building a Linux-based virtual machine with Parrot Linux to perform various tasks, such as port scanning, quick high-level vulnerability assessments (primarily to verify a single vulnerability on one or more systems, validate that McAfee services were functional, or verify that a patch had been applied).
    - Performing network packet capture and traffic analysis using both Wireshark and tcpdump/windump.
- Perform troubleshooting for various network performance and connectivity issues related to both McAfee versions, VSE and ENS. Primarily troubleshooting WAN circuit saturation issues, firewall issues, various "port unreachable" errors, and network routing issues related to the Ascension WAN and VPN.
- Work with the Application Packaging Team to assist in automating the process of loading their applications into the GTI file reputation database. This included developing the trusted internal certificate management process mentioned previously, along with testing the code signing process and providing demonstrations to various members of the Application Packaging Team.
- Work with members of both the Server and Workstation teams to troubleshoot system performance issues related to McAfee ENS. This includes using various McAfee-provided utilities, such as ENS Profiler, AMTrace, and GetClean, along with 3rd party utilities such as ProcMon and other utilities from the SysInternals suite of applications, and Microsoft-provided utilities, such as the Windows Performance Recorder.
- Assist in the migration of McAfee ePolicy Orchestrator (ePO) to new hardware and upgrading ePO from 5.3 to 5.9. This includes rebuilding Agent Handler systems and software repositories for all ministries within Ascension.
- Assist with database issues related to the McAfee ePO database server, Microsoft SQL Server 2016 Enterprise. This includes aiding the Database Administration Team during the migration to the new hardware and assisting with performance issue troubleshooting.

Consultant
St. Charles Engineering & Surveying, Inc.
February 2017 – October 2017

- Under contract to develop an in-house Project Management software solution, utilizing the Microsoft development stack (C#, SQL Server, and IIS).
- The application is used to manage time for both billable and overhead time. Each unique commercial job is entered into the

system as a Project, and all employee time is tracked through the application, billable and overhead.
- Responsible for all Level 2 and 3 support issues, including Windows Server and Microsoft Exchange administration, Linux server administration, firewall administration, and information security auditing, configuration changes, and system maintenance pertaining to security issues.

Senior Information Security Analyst
UniGroup, Inc.
October 2015 – February 2017

- Perform vulnerability scanning and penetration testing utilizing the Nexpose and Metasploit application platforms.
- Develop a standardized process for scanning enterprise information assets, covering both discovery and vulnerability scanning, as well as penetration testing.
- Develop a web-based application utilizing the Ruby programming language and the Ruby on Rails web framework to integrate vulnerability findings from the Nexpose scanner with the ServiceNow incident management platform. The application integrates the APIs from both platforms, allowing incident tickets to be created and managed in ServiceNow based on scan results from Nexpose.
- Work with members of the server and network teams to develop a standardized process for vulnerability identification and remediation.
- Administer and maintain the McAfee Enterprise Security Manager SIEM product. This includes adding and removing data sources, verifying configuration, and updating the product.
- Begin preparation for ISO 27001 certification, including document review and classification.
- Design an internal web-based application to track required ISO documentation, ISO 9001:2008 certification, for presentation to external ISO auditor.
- Administer and maintain the Symantec Endpoint Client security product enterprise wide. This includes migration to a new management server platform and upgrading all endpoint clients in order to resolve a major security vulnerability within the Symantec client.
- Develop multiple Windows Powershell scripts to perform various administrative tasks, including enumerating active Microsoft Exchange accounts.

Information Security Analyst
Mallinckrodt Pharmaceuticals
Sep. 2014 – Sep. 2015

- Administer and maintain the Splunk enterprise logging platform globally, including application and system upgrades, custom report design, real-time alert management, and log forwarding configuration as new systems were deployed to production.
- Administer and maintain F5 BIG-IP appliances, operating in a reverse proxy configuration, protecting multiple DMZ networks in the headquarters data center. Responsible for all F5 configuration, including working with members of the Web team to implement policy for new sites/servers as they're brought online in production.
- Responsible for all vulnerability scanning, using the Nessus scanner software. This includes working with other groups within

the enterprise to remediate vulnerabilities discovered as a result of the scans, development of a scanning schedule to satisfy external audit and internal requirements, scan profile development and maintenance, and application and operating system updates on the scanning systems (running Debian Linux).

- Administer and maintain the Sourcefire intrusion prevention system (IPS) globally. Completed a project in April 2015 to upgrade the Sourcefire software from version 4.0 to version 5.0 on the Defense Center and all 3D Sensors. The scope of the project included a bottom-up redesign of the Intrusion and System policies in place, and implementation of traffic blocking (prior to the upgrade, the system had been in monitor only mode).
- Subject matter expert (SME) for the Linux operating system. This includes making recommendations regarding standard builds for the various Linux distributions in production, helping to fully integrate system monitoring for all Linux systems, and providing troubleshooting assistance to other teams when needed.
- Administer and maintain the Websense Internet monitoring platform globally. Work with the legal department as part of the decision-making process for site access requests internally.
- Administer and maintain the SecureLink application for remote vendor access, including new account creation, troubleshooting, and interfacing with the vendor to request new features on multiple occasions.
- Administer and maintain the AlgoSec Firewall Analyzer software application. The software provides daily reports on all enterprise firewall rule and configuration changes and real-time alerting for certain change types.
- Participate in the design and implementation of the Mallinckrodt internal Windows Certificate Authority servers/services. Participate in the administration and maintenance of these systems going forward. Responsible for issuing all internally signed certificates where the purpose of the certificate was application signing/web site security.
- Administer and maintain the Microsoft BitLocker Administration Console to retrieve lost BitLocker keys enterprise-wide, along with troubleshooting BitLocker key generation/retrieval issues.
- Review and issue external SSL certificates for the Mallinckrodt.com domain (among other domains owned by Mallinckrodt and managed internally) using the web based Comodo Cert Manager Web application. This includes generating the Certificate Signing Request (CSR) for domain entries as needed, converting from Microsoft PKCS12 format to OpenSSL PEM format when needed), and retrieving, validating, and delivering the completed certificate chain to the end user.

Systems Director
Worldwide Freight Management
Oct. 2006 – Sep. 2014

- Responsible for all aspects of Information Technology, including networking, server, and desktop/laptop support, maintenance, and troubleshooting.
- Install, configure, and maintain Microsoft Exchange Server 2010 environment, including server-based antispam and antivirus filtering.
- Install, configure, and maintain multiple corporate firewalls, utilizing the pfSense firewall platform, providing Internet access, dedicated remote site VPN (virtual private network) connectivity, and remote user access to the corporate network.
- Implement data backup procedures (both on and offsite) for all corporate data including documents stored on shared network

drives, email data, web site files, programming source code, and application databases.

- Develop a new web-based project management application, based on features present in an existing legacy application, as well as new business requirements. The application utilizes the Microsoft C# programming language, Microsoft ASP.NET web technology platform, and Microsoft SQL Server database platform for data storage.
- Develop a Transportation Management System (TMS) web-based application interface to various carrier API's (Application Programming Interfaces) in order to provide real-time price quotes, shipment tracking, and document retrieval. The application utilizes the Microsoft C# programming language, Microsoft ASP.NET web technology platform, and Microsoft SQL Server database platform for data storage.

Senior Information Security Analyst
MasterCard International
Feb. 2005 – Oct. 2006

- Responsible for all aspects of security monitoring, including network- and host-based Intrusion Detection systems and Security Information Management systems.
- Re-architect existing Intrusion Detection systems platforms (host and network) in order to improve performance, increase coverage, and provide a higher degree of visibility.
- Perform computer forensic investigations at the request of multiple departments.
- Responsible for enterprise vulnerability management across all network and security devices, operating systems, and enterprise applications.
- Influence policy decisions and developed policy and procedural documentation for security monitoring, computer forensics, incident response, and vulnerability management.
- Responsible for the analysis, selection, and implementation of a third-party 24x7 security monitoring solution to augment the existing operational monitoring environment.
- Assist in the completion of GLBA, SOX 404, FFIEC, and internal audit compliance items, as needed.
- Assist in vulnerability assessments and penetration testing, as needed.

Manager of Security Services
TechGuard Security, LLC
Oct. 2003 – Feb. 2005

- Perform penetration testing and vulnerability assessments for commercial customers on both a project-based and recurring basis.
- Implement enterprise security policies and procedures based on recognized best practices, such as NIST and NSA standards.
- Perform forensic analysis at both the system and application level.
- Implement, monitor, and maintain managed Intrusion Detection systems for commercial customers and the internal corporate LAN, utilizing the Snort IDS package on Linux.
- Provide external management of customer networks containing a combination of Windows NT/2000/2003, Sun Solaris, HP-UX, and Red Hat Linux operating systems and Cisco networking equipment.
- Audit, securely configure, and maintain Cisco routers for vulnerability assessment and network management purposes for commercial customers, as well as the corporate network, using the router audit tool (RAT) from the Center for Internet Security as a baseline.

- Perform security auditing and system administration for customer-owned HP-UX and SCO Unix systems, including network services configuration (inetd, sendmail, etc.), application troubleshooting and auditing, user and group authentication configuration, and file uid/gid ownership configuration.
- Implement, maintain, and troubleshoot both customer-owned and managed firewalls, including Linux-based firewalls, Cisco PIX firewalls, SonicWall firewalls, NetScreen firewalls, Watchguard firewalls, and Cisco routers. This includes firewall rule set modification and maintenance, VPN tunnel and client connectivity setup and troubleshooting, service availability issues, traffic shaping/quality of service issues, external penetration testing, and updates.
- Monitor and maintain commercial customer WAN environments, troubleshoot IP routing issues, and perform infrastructure upgrades and audits.
- Implement and audit Windows 2000 and 2003 Active Directory, including site migration from Windows NT, using SANS and NSA standards as a guideline.
- Implement system and network monitoring using the open-source application Big Brother for both the internal corporate LAN and managed customer systems and networks.
- Implement centralized Windows patch management using Microsoft Software Update Services for the corporate LAN, and Microsoft Software Update Services and Shavlik HFNetChk Pro for commercial customers.
- Assist in the development of corporate policy and procedure documentation relating to information security, change management, incident handling, and access control.
- Implement. maintain, and monitor file integrity applications, such as the open-source applications Tripwire and Samhain, on all corporate Linux systems using the open-source utility.
- Implement and maintain OpenSSH public-key authentication for all corporate Linux systems and managed commercial systems. Responsible for maintaining private key backup repository for all engineers and developers.
- Assist in the development of policy and procedure documentation for commercial customers as it relates to acceptable use, security, and access control.
- Audit security configurations for both internal and commercial customer Wireless LAN's (WLAN's), both 802.11a and 802.11b. Configure and deploy WEP and WPA for commercial business customers.
- Responsible for implementation, configuration, and maintenance of the corporate web environment, Apache 2.0 on Linux operating system.
- Perform secure configuration of the corporate web environment, including mod_security configuration, Apache configuration hardening according to industry-standard best practices, and PHP security configuration.
- Perform quarterly audits of corporate web environment using open-source tools such as Nessus and Nikto, and custom scripts, primarily focusing on server mis-configuration, SQL injection vulnerabilities, cross-site scripting vulnerabilities, input validation errors in web site code, and operating system/application level vulnerabilities (such as vulnerabilities in Apache/PHP).

- Audit web application code (PHP and Java languages), examining code for logic errors, input validation flaws, and other potential errors.
- Perform quarterly security audits of all internal systems using open-source tools, such as Nmap and Nessus, and custom scripts.

Information Security Manager
Quick Study Radiology
Aug. 2001 – Oct. 2003

- Configure, secure, and maintain production web application environment running Apache 1.0-series on IBM's AIX operating system.
- Responsible for all enterprise security auditing, including logging structure, access control, password policies, Active Directory group policy, network device configuration, client/server application security, web application security, database configuration, operating system configuration and patch maintenance, and internal and external penetration testing.
- Evaluate both internal and customer systems and networks for compliance with HIPAA guidelines and recommendations.
- Perform enterprise firewall and VPN administration, including maintenance and monitoring of the logging and alerting environment, ingress and egress protocol filtering implementation and maintenance, and remote connectivity for employees, customers, and business partners.
- Implement, configure, maintain, and monitor the Snort IDS application on Linux. This includes rule set updates, response to incidents, and configuration relating to the internal LAN/WAN environment.
- Implement, configure, and maintain enterprise system and network monitoring using open-source tools and custom developed applications.
- Integrate business process automation scripts, intranet applications, issue tracking, and customer relationship management applications to provide a seamless data flow across business units.
- Develop and implement information security and technology acceptable use policies, access control policies, and remote access policies for corporate headquarters employees, billing operations employees, and customer sites.
- Perform Unix system administration on the Sun Solaris, Red Hat Linux, and AIX operating system platforms.
- Perform network administration including Cisco routers and switches and corporate ATM WAN.
- Implement, maintain, and monitor file integrity on all corporate Linux systems using the open-source utilities Samhain and Tripwire.
- Implement OpenSSH public-key authentication for all internal Linux and Unix systems. Integrate Linux passwd databases with Microsoft Active Directory using Kerberos and OpenLDAP.
- Perform quarterly audits of all Cisco routers in the corporate ATM WAN, using the router audit tool (RAT) from the Center for Internet Security as a baseline.
- Implement centralized Windows patch management using Microsoft Software Update Services for all corporate workstation and server systems.
- Implement and maintain secure wireless networking for the St. Louis headquarters location, utilizing the 802.11b standard. This

included the implementation and maintenance of 128-bit WEP and MAC address filtering.

Senior Network Administrator
Vertecon, Inc.
Apr. 2000 – Jul. 2001

- Perform enterprise firewall and VPN administration.
- Responsible for all internal and external penetration testing and vulnerability assessments.
- Implement, configure, maintain, and audit Windows 2000 Active Directory.
- Perform IBM WebSphere implementation, administration, and auditing.
- Implement, configure, and maintain IBM WebSphere development environment on Sun Solaris operating system.
- Monitor and maintain IBM's DB2 and Oracle 8i database development environments on Sun Solaris.
- Develop procedures for quality assurance and data recovery when moving code between development, staging, and production web environments.
- Manage encryption technologies, including securing email and encrypted file systems using S/MIME and PGP, and securing both development and production web sites using SSL encryption.
- Administer development and managed hosting environment using servers running Sun Solaris and Red Hat Linux.

IT Specialist
Shandwick International
Mar. 1999 – Apr. 2000

- Support approximately 60 users in the St. Louis location, including desktop support, file and print services, email services, domain authentication, dial-in services, and phone system.
- Develop annual IT budget and maintain vendor relationships.
- Develop and implement information security and technology acceptable use policies.

Consultant for Client
SBC Communications
Jul. 1998 – Mar. 1999

- Provide support in a Microsoft Windows NT server-based network, with Windows NT 4.0, Windows NT 3.51, OS/2, Windows 95, Windows for Workgroups, and Winframe clients.
- Administer user accounts and group accounts on multiple domains.
- Provide support for Microsoft Exchange and MS Mail, as well as various Telnet and host access platforms (including Chameleon, SmarTerm, Exceed, and Windows 95/NT Telnet).
- Provide support for Microsoft Office 95/97 products, and Internet Explorer and Netscape Navigator Internet access programs.

Consultant for Client
Brooks Fiber/MCI Worldcom
Oct. 1997 – Jul. 1998

- Provide support for approximately 2,000 users nationwide and approximately 400 users locally in a 90% Windows NT networking environment with Microsoft Exchange Server, and 10% Novell networking environment with a GroupWise mail platform.
- Administer user and group accounts on one Windows NT domain on a Windows NT server-based network. Responsible for creating new accounts, removing expired accounts, and administering group access to servers and disk shares.

Consultant for Client
Unity Health Systems
Jul. 1997 – Oct. 1997

- Worked on a rollout of approximately 2,000 new IBM desktop PC's.

Professional Achievement

2005 - SANS Institute Local Mentor, GIAC Certified Perimeter Protection Analyst (GPPA) Certification Program - http://www.giac.org/certification/certified-perimeter-protection-analyst-gppa

- Mentored 25 people in a week-long class to prepare them for the GPPA certification exam, including preparation of multiple hands-on lab exercises based on the course material, and oversight of a practice exam at the conclusion of the course.

SANS Certifications Held:

- GIAC Certified Intrusion Analyst (GCIA) – 2006 – 2010 (Analyst #6840)
- GIAC Perimeter Protection Analyst (GPPA) – 2002 – 2010 (Analyst #351)
- GIAC Security Essentials (GSEC) – 2002 – 2008 (Analyst #1421)
- Personal URL: https://www.giac.org/certified-professional/matt-pogue/102674

Education

DeVry Institute of Technology 1996 - 1997
Electronics Engineering Technology, Kansas City, MO
Studies focused on electronics engineering and circuit design. Two semesters completed.

Mineral Area College 1995 - 1996
General Courses, Park Hills, MO
General study courses. Approximately 60 credit hours completed.