Matthew Straub

Information Security Engineer

Contact

Phone
618-340-5859

E-mail
Matthew_Straub@outlook.com

LinkedIn
https://www.linkedin.com/in/matthew-straub1/

Portfolio
https://matthews-homelab.com/

Skills

• Microsoft Purview, Netskope, Kibana, Splunk, F-Secure / WithSecure Elements, Proofpoint, CrowdStrike, Xsoar, E-Discovery
• Windows Server, Active Directory, Network Security

• PRTG / Network Management Systems

• DHCP, DNS, IIS, VPNs

• CMD, PowerShell, Bash, SQL

• Linux, Windows

• Azure, Defender 365, Compliance, DLP

• Exchange Server (EAC), VMWare, Hyper-V

• Cisco Meraki, Palo Alto

Ambitious and passionate Engineer with ample hands-on experience in bleeding-edge and industry-standard technologies. A skilled communicator always innovating to find unique solutions to complex problems.

Work History

2024-01 – Current

Information Security Engineer

World Wide Technology, St. Louis, Missouri

- Orchestrate enterprise-wide Data Loss Prevention (DLP) controls using Microsoft Compliance / Purview, CrowdStrike and Netskope, curate numerous policies and procedures to protect the organization's data and assets – collaborate directly with internal IT and leadership teams to drive information protection initiatives.
- Deploy, configure, and maintain data protection tools, policies, and technologies to monitor, detect, and prevent data leakage, data exfiltration and unauthorized data transfers using Microsoft Compliance, CrowdStrike and Netskope.
- Design comprehensive controls to detect, monitor and mitigate insider threats to the organization using Microsoft Compliance / Purview Insider threat policies.
- Implement eDiscovery solutions to mitigate litigation across the organization's 10,000+ employees located around the world using Microsoft Purview.

2023-03 – 2024-01

IT Security Administrator

Zoltek Corporation, subsidiary of Toray, St. Louis, Missouri

- Orchestrate and manage Palo Alto firewalls, VeloCloud SD-WANs, Global Protect VPN gateways, Meraki and Cisco routers, switches, and access points across global network of 10+ locations.
- Implement security procedures and ensure global compliance and best-practices of policies across thousands of users and endpoints in 3+ countries using Azure endpoint management, Microsoft Intune, Microsoft 365 Defender, and F-Secure / WithSecure Elements.
- Design Microsoft Defender 365 email & collaboration and compliance policies for DLP and threats (Anti-Malware, Anti-Spam, Bulk-Email, Anti-Phishing, DLP etc.)

2022-05 - 2023-03

IT Systems Engineer

Primary Systems, St. Louis, Missouri

- Manage installation, deployment, maintenance, configuration and troubleshooting of Windows Server, SQL Server, VMware, Active Directory, IIS, Linux, Exchange, Paessler Router Traffic Grapher (PRTG) and Azure environments at <u>enterprise scale.</u>
- Develop solutions to automate and simplify operations via Power Shell, CMD and SQL. Implement DevOps solutions across organization to <u>trim overhead</u> and increase department efficiency. Developed Power Shell toolkit to automate migrations which <u>saves 100+ hours yearly.</u>
- Deploy networks, workstations, printers, VPNs, DNS, DHCP, WSUS, servers, Barracuda, Trend Micro, and Active Directory across <u>numerous organizations.</u>

2021-05 - 2022-05

IT Systems Analyst

Primary Systems, St. Louis, Missouri

- Install, deploy, maintain, configure, and troubleshoot Windows Server, SQL Server, VMware, Active Directory, Linux, and Exchange at <u>enterprise scale.</u>
- Performed 15+ migrations and upgrades of hospital's life-safety systems utilizing SQL, Windows Server, IIS, and PowerShell.
- Deployed workstations, printers, VPNs, DNS, DHCP, and Active Directory internally.

Education

2024-04 – 2024-06

Master of Science: Information Technology Management

Western Governors University - Salt Lake City, UT

2022-10 - 2023-12

Bachelor of Science: Information Technology

Western Governors University - Salt Lake City, UT

2019-08 - 2021-05

Associates of Technology: Information Technology

Ranken Technical College - St. Louis, Missouri

Certifications

- ISC2 CISSP
- Microsoft Certified: Information Protection and Compliance Administrator Associate
- AWS Certified Cloud Practitioner
- LPI Linux Essentials
- CompTIA Security +
- CompTIA IT Operations Specialist
- CompTIA Secure Infrastructure Specialist
- CompTIA Network+
- CompTIA A+
- ITIL 4 Foundation
- Microsoft Certified: Azure Fundamentals
- MTA: Windows Server Administration Fundamentals

Projects

- [SIEM and XDR / Anti-Virus](#)
  - Deployed an enterprise SIEM and XDR / Anti-virus using Wazuh.
- [LearnPython Project](#)
  - Developed a Python learning challenge.
- [Windows Troubleshooting Collector](#)
  - Developed a PowerShell toolkit to troubleshoot common Windows errors.
- [Ubiquiti Dream Machine](#)
  - Deployed an enterprise switch, router & firewall solution using Ubiquiti.
- [Pi-Hole](#)
  - Implemented a comprehensive recursive DNS, DHCP & ad blocking solution using Pi-Hole.
- [Portfolio](#)
  - Created an intricate portfolio utilizing WordPress.
- [Dell Server](#)
  - Deployed active directory, DNS, DHCP, IIS and ESXI.
- [Synology NAS](#)
  - Implemented a redundant NAS & media center utilizing Synology.