

# < Holden Prather >

270.519.9816 | Jprather223@gmail.com | [MySite](#) | [LinkedIn](#)

## EXPERIENCE

### Cyber Security Specialist

Computer Services, Inc. (CSI)

Oct. 2023 - Apr. 2025

Paducah, KY

- **Bot Mitigation & Web Application Security:** Spearheaded the migration of critical applications to Akamai Kona (WAF) and Bot Manager. This initiative slashed bot traffic by over 90% on core services and significantly bolstered protection against OWASP Top 10 vulnerabilities.
- **Firewall Modernization & Automation:** Developed and implemented automation processes to seamlessly transition Cisco ASA firewalls to next-generation Cisco FTD devices in live production environments. This approach ensured a smooth migration, reduced downtime, and minimized errors.
- **DevSecOps Leadership:** Championed DevSecOps principles to integrate security seamlessly into the CI/CD pipeline and advised DevOps and Development teams on best practices.
- **Azure Network Transformation:** Led a complex migration from a Legacy Azure hub-and-spoke environment to a modern Azure Virtual WAN (VWAN) hub model, improving scalability and security.
- **Web Content Filtering Innovation:** Conducted multiple proof-of-concept (POC) projects to design a scalable, cloud-managed web content filtering solution for tens of thousands of ISP customers.
- **Incident Response & Vulnerability Management:** Provided escalation support for the incident response team, wrote custom WAF and IPS rules, and proactively performed vulnerability remediation using tools like NMAP, Burp Suite, Qualys, and Nessus.
- **Security Monitoring & Log Analysis:** Leveraged SIEM platforms (RSA NetWitness and Splunk) to conduct in-depth log/packet analysis, significantly reducing time spent on incident response.

### Network Operation Engineer

Computer Services, Inc. (CSI)

Mar. 2020 - Oct. 2023

Paducah, KY

- **Network Design & Security:** Designed and implemented secure network infrastructure (LAN, WAN, firewalls, VPNs, SD-WANs) for 70 unique financial institution environments while maintaining uptime for over 400 others.
- **Infrastructure Automation & DevOps:** Drove the adoption of automation tools like Ansible, Terraform, and Azure DevOps and implemented version control systems (Git) for code and configuration integrity.
- **Network Visibility & Automation:** Deployed IP address management systems to achieve 100% visibility across a hybrid environment.
- **Enterprise Systems Administration:** Managed and optimized critical enterprise infrastructure systems.
- **DNS Expertise & Load Balancing:** Administered a large-scale distributed DNS environment (RHEL, Infoblox) and implemented DNS Load balancing using F5 BIG-IP DNS.
- **Vulnerability Management:** Proactively reviewed and resolved CVEs to maintain network security.

## Skills Summary

### Vendor Specific

- Cisco Systems Products
  - Adaptive Security Appliance (ASA)
  - Advanced Malware Protection (AMP)
  - Aggregation Services Routers (ASR)
  - Cisco Application Policy Infrastructure Controller (APIC)
  - Firepower Threat Defense (FTD)
  - Intrusion Detection Prevention systems (IDPS)
  - Meraki
  - StackWise
  - Umbrella (OpenDNS)
  - Unified Communications Manager (CUCM)
  - Unified Computing System (UCS)
- F5
  - BIG-IP Centralized Management
  - BIG-IP Global Traffic Manager (GTM)
  - BIG-IP Local Traffic Manager (LTM)
- RSA Cyber Security
  - RSA NetWitness
  - RSA SecureID
- Solarwinds
  - N-able (N-Central)
  - Orion
- VMware
  - ESXi
  - vSphere
- Akamai Kona (WAF)
- Archer GRC Solution
- Autotask ITIL
- Cloud Access Security Broker (CASB)
- Forcepoint Content Filtering
- GitHub
- Infoblox
- Microsoft Azure
- ServiceNow ITIL
- Splunk
- Symantec Security
- Terraform by HashiCorp

### Technical Skills

- Governance
  - General Data Protection Regulation (GDPR)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Payment Card Industry Data Security Standard (PCI DSS)
- Networking
  - Cloud Networking
  - DNS Administration
  - Infrastructure as Code
  - Network Engineering
  - Network Orchestration
  - SD-WAN
  - Traffic Management And Load Balancing
- Security
  - Cloud Security
  - Website Security
  - DDoS Mitigation
  - Email Security
  - Information Security
  - Internet Security
  - Network Security
  - Penetration Testing
  - Security Information and Event Management (SIEM)
  - Security Orchestration Automation and Response (SOAR)
- Platforms
  - Linux Administration
  - Microsoft Azure
  - Window Active Directory
  - Window Administration
- Programming
  - Python
  - Bash
  - C
  - Powershell
  - Representational State Transfer (REST-API)
  - HTML, CSS, JavaScript