<Holden Prather>

Architect | Developer | Engineer

--about-me

IT Engineering professional with 5 years of experience within the highly regulated financial industry. A proven history of successfully designing, building & securing business critical assets and services within a complex hybrid environments. Life-long learner with a passion for technology and a drive to stay ahead of the curve. Currently pursuing the Offensive Security Certified Professional (OSCP) certification.

--work-experience

Computer Services, Inc. (CSI) | Cyber Security Specialist
October 2023 - Present

- **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 automation approach not only ensured a smooth migration but also reduced downtime and minimized the risk of errors.
- **DevSecOps Leadership:** Championed DevSecOps principles to integrate security seamlessly into the CI/CD pipeline. Actively advised DevOps and Development teams on best practices for a cohesive and secure cloud environment.
- **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 and reporting for the incident response team. Wrote custom WAF and IPS rules to mitigate observed malicious traffic. Proactively performed vulnerability remediation using tools like NMAP, Burp Suite, Qualys, and Nessus. This minimized downtime, improved network performance, all while keeping within compliance.
- **Security Monitoring & Log Analysis:** Leveraged SIEM platforms (RSA Netwitness and Splunk) to conduct in-depth log/packet analysis and investigations across various sources. This significantly reduced time spend on incident response and mitigation.

Computer Services, Inc. | Network Operation Engineer
March 2020 - October 2023

- **Network Design & Security:** Designed and implemented secure network infrastructure solutions, including LAN, WAN, firewalls, VPNS, SDWANS, Cloud and other components, for 70 unique environments to meet the unique security and performance requirements of financial institutions while maintaining uptime for over 400 others.
- **Infrastructure Automation & DevOps:** Drove the adoption of automation tools like Ansible, Terraform, and Azure DevOps to streamline infrastructure management, improve efficiency, and reduce manual effort. Implemented version control systems (CVS, SVN, Git) to ensure code and configuration integrity.
- **Network Visibility & Automation:** Deployed IP address management systems to achieve 100% visibility across a hybrid environment, enhancing inventory management and compliance.
- **Enterprise Systems Administration:** Managed and optimized critical enterprise infrastructure systems including ensure peak performance and reliability.
- **DNS Expertise & Load Balancing:** Administered a large-scale distributed DNS environment across RHEL and Infoblox platforms, overseeing hundreds of zones. Implemented DNS load balancing using F5 BIG-IP DNS to optimize performance and resilience.
- **Vulnerability Management:** Proactively reviewed CVEs assessing their potential impact and implementing appropriate resolutions to maintain network security and uptime.

West Kentucky and Tennessee Telecommunications (WK&T) | Technical Support
November 2018 - March 2020

- **Technical Support:** Provided expert technical support to customers via phone and onsite visits, resolving a wide range of issues related to phone, TV, and internet services.
- **Technical Guidance & Troubleshooting:** Patiently guided customers through equipment installation and troubleshooting processes, ensuring they could successfully use their services.
- **Dispatch & Logistics Optimization:** Efficiently coordinated and dispatched field technicians to onsite appointments, minimizing travel time and maximizing productivity.
- **Computer Repair & Optimization:** Offered additional value to customers by providing computer repair services, including part replacement, virus removal, and performance optimizations.

--certifications

- ACTIVELY PURSUING - Offensive Security Certified Professional (OSCP)
- 2024 - Traffic Management Operating System (TMOS)
- 2023 - Microsoft Certified: Azure Fundamentals (AZ 500)
- 2020 - Cisco Certified Network Associate (CCNA)

--skills-summary

Vendor Specific

- Akamai Kona (WAF)
- Archer GRC Solution
- Autotask ITIL
- 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)
- Cloud Access Security Broker (CASB)
- F5
  - BIG-IQ Centralized Management
  - BIG-IP Global Traffic Manager (GTM)
  - BIG-IP Local Traffic Manager (LTM)
- Forcepoint Content Filtering
- GitHub
- Infoblox
- Microsoft Azure
- RSA Cyber Security
  - RSA NetWitness
  - RSA SecureID
- ServiceNow ITIL
- Solarwinds
  - NAble (NCentral)
  - Orion
- Splunk
- Symantec Security
- Terraform by HashiCorp
- VMware
  - ESXi
  - vSphere

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
  - SDWAN
  - 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
  - Bash
  - C
  - Powershell
  - Python
  - Representational State Transfer (REST-API)
  - Terraform