Paxton Patronas

paxtonpatronas@gmail.com | linkedin.com/in/paxtonpatronas/ | paxtonpatronas.com

Experience

SOC Analyst Internship June 2025 – August 2025
Ford Office Technologies *Conellsville, PA*

- Analyzed and evaluated 400+ alerts in Endpoint Detection and Response (EDR) system, reducing false positives and improving threat response efficiency.
- Introduced to Security Information and Event Management (SIEM) through incidents, developing a basic understanding of an Incident Response Procedure (IRP).
- Audited 90+ passwords from multiple system administrators, remediating non-compliant passwords to improve security.

Information Technology Internship February 2025 – April 2025
First United Bank & Trust *Oakland, MD*

- Observed IT professionals, developing a better understanding of cybersecurity practices, network administration, and troubleshooting.
- Assisted staff with on-sight operations and carrying physical objects, reducing time and improving efficiency.
- Learned about Active Directory, Provision (database management), and ticketing system, gaining exposure to enterprise technologies.
- Labeled and repackaged 80+ check scanners for company usage, enabling main IT staff productivity.

Projects

Home Lab | *Systems Administration, Virtualization, Networking* September 2024 – Present

- Maintain and utilize a Proxmox cluster with various services (local DNS, Samba NAS, VPN), simulating a professional infrastructure.
- Implemented multiple virtual machines and Docker containers, improving resource utilization and efficiency.
- Configured firewall rules and VLAN segmentation through pfSense VM, protecting and securing home network.

SIEM Environment | *Monitoring, Threat Hunting, Incident Response* August 2025 – November 2025

- Utilized SPAN mirror port on network switch to monitor LAN network traffic, acknowledging and escalating alerts from network-based intrusion detection system (NIDS).
- Integrated pfSense Snort interface with Emerging Scan rules on WAN, analyzing possible port scans to identify and report malicious IP addresses.
- Simulated attack on an endpoint machine, correlating host events and network detections to threat hunt and build a case.

Relevant Skills

Operating Systems: Windows, Linux
Virtualization & Containerization: Hypervisors, KVMs, Docker
Network Security: DNS, DHCP, VLANs, VPNs
Ethical Hacking: Kali, Metasploit, Wireshark
Hardware: Deployment, Troubleshooting, Management
Collegiate Baseball: Communication, Self-discipline, Collaboration

Certifications

COMPTIA Network+: November 2024 - 2027
COMPTIA Security+: August 2024 - 2027

Education

Indiana University of Pennsylvania Indiana, PA
Bachelor of Science in Computer Science, Minor in Criminology *August 2025 – May 2027*

Garrett College McHenry, MD
Associate's of Applied Science in Cybersecurity *August 2023 – May 2025*