BRENNAN VIGNA
586-741-9647 | bvigna42@gmail.com |
Waterford, Michigan

EXPERIENCE

Sehi Computer Products | IT Support Analyst
10/2023 – Present

- Investigate and triage endpoint, account, and security alerts using endpoint protection tools, Windows Event Logs, and Active Directory.
- Provide technical support for Windows systems, user accounts, and network connectivity issues while maintaining security best practices.
- Analyze phishing emails and suspicious activity by reviewing headers, URLs, attachments, and user behavior; document findings and coordinate remediation with senior IT staff.
- Assist with system hardening and vulnerability reduction by reviewing configurations, patch status, and endpoint alerts in collaboration with system administrators.

Sehi Computer Products | IT Intern / IT Support
09/2021 – 08/2023

- Maintained high availability of wireless and wired networks by troubleshooting DHCP, DNS, and connectivity issues
- Supported onboarding and access provisioning for 50+ users through Active Directory and Microsoft 365 administration

EDUCATION

- Bachelor of Science in Information Technology – Expected June 2026

  Walsh College School of Technology | Cybersecurity
- Associate Degree in Computer Information Systems – Cybersecurity

  Oakland Community College | Dean's List

SECURITY PROJECTS & HANDS-ON EXPERIENCE

Enterprise Blue Team Security Labs

Windows Server | *Linux* | *Security Onion* | *Wireshark*

- Hardened Windows Server and Linux systems by auditing users, services, scheduled tasks, firewall rules, and local security policies to establish secure baselines
- Performed static PCAP analysis in Wireshark to identify malicious traffic, carve malware payloads, compute file hashes, and validate findings using OSINT tools
- Investigated suspicious network activity using Wireshark, netstat, TCPView, DNS/WHOIS lookups, and sandbox analysis to differentiate benign from malicious behavior
- Analyzed IDS alerts in Security Onion and correlated network indicators with host-level artifacts to support incident triage and detection workflows

SOC Detection & Monitoring Projects

- Built ELK pipeline ingesting Windows Sysmon logs; created dashboards and detection logic for failed logons and anomalous process activity

- Deployed Suricata on pfSense and integrated alerts into ELK to detect reconnaissance and lateral movement patterns
- Created a mock incident response workflow including alert enrichment, analysis, documentation, and escalation

TECHNICAL SKILLS

- Tools: PowerShell, Splunk, pfSense, Suricata, Wireshark, Sysmon, Windows Defender, ELK Stack
- Languages/Scripting: PowerShell, Python
- Security Concepts: Incident response, alert triage, threat analysis, SOC workflows, phishing investigation, system hardening, network monitoring
- Operating Systems: Windows, Linux (Ubuntu/Kali)
- Vulnerability Assessment