Brett Szpont

586-719-7534 | **szpontb@gmail.com**| Detroit Metro Area | brettszpont.com

OVERVIEW

Cyber security professional with experience in threat hunting and incident response which includes determining how an environment has been compromised and perform appropriate actions to build back the client's environment. Strong ability to communicate with clients to define clear objectives and build long lasting partnerships. Driven by continuous improvement and always staying up to date with the latest security trends. Consistently advancing my knowledge with training courses and certifications.

EDUCATION

Baker College: Charter Twp of Clinton, MI (Currently Attending)
Major: Information Technology and Security - Concentration in Information Assurance and Cyber Security

EXPERTISE

Microsoft 365 | Malware Analysis | Continuous Improvement | Virtual Machine Setup/Maintenance/Configuration | Linux OS | Proficient with Kali Linux | Virtual Private Servers | AWS | T-Pot Honeypots | Customer Satisfaction | Threat Hunting | Social Engineering | Elastic | CrowdStrike | Malicious Domain Monitoring | Palo Alto Firewalls| Fortinet FortiGate Firewalls | Incident Response | OSINT

PROFESSIONAL EXPERIENCE

Security Consultant
N1 Discovery | Troy, MI | MAR 2022 – PRESENT

- Monitored for malicious domains that were recently registered and attempt takedowns with registrars.
- Ensure that an environment is locked down and off the network during a cyber incident – investigate and locate the root cause of the specific breach – remediate and build back the environment.
- Frequently use SIEM software such as Splunk or Elastic for log analysis and data slinging.
- Creating polices/rules using EDR software for client environments which include alerts , generating workflows , threat hunting , and scheduling patches.
- Take part in social engineering experiments that included on-site testing/phishing attempts.
- Perform Microsoft 365 assessments in tenant environments/run internal and external vulnerability assessments.
- Performed firewall maintenance such as reviewing traffic, opening/closing ports, monitoring web traffic, create DNS filters.
- Monitor dark web for any recent leaks of PII including names, addresses, usernames, and passwords.

Security Consultant/Information Technology Consultant
Falcon Network Services | Troy, MI | NOV 2019 – MAR 2022

- Manages companies Security SIEM tools to ensure all systems are secure from any unauthorized use, malware infections, and other problems that would compromise sensitive information.
- Configures and deploys computers, servers, and other equipment to clients.
- Assists in security risk assessments.
- Monitor all logs as well as pinpoint/remove all viruses on the compromised systems.
- Maintain awareness of cyber trends, threats, and new vulnerabilities.
- Understanding the client's needs and giving them optimized results.
- Assists software installation as well as deployment.
- Neatly documents installation processes as well as other given tasks for clients' future reference.
- Create custom images and deploy to companies' computers.
- Remotely access hardware and software for clients to make changes and correct problems.
- Diagnosing system errors and other issues.

Team Lead
Wolf Window & Screen Repair | Charter Twp of Clinton, MI | OCTOBER 2016 – NOV 2019

- Maintained company website, Google business page, and scheduling software.
- Delivered and installed newly fabricated glass and window screens.
- Evaluated potential jobs and prepared customer estimates.