JASON BURNS

Cyber Security Expert

Contact

Address
Scranton, PA, 18444

E-mail
Jason.Burns92.jb@gmail.com

LinkedIn
https://www.linkedin.com/in/jason-burns-294967118/

Skills

- Incident Response Management — Excellent
- Security Automation Engineering — Excellent
- Threat Research/Hunting /Emulation — Excellent
- Compliance Auditing — Excellent
- Linux/Unix/Windows Security & Forensics — Excellent
- SOC Management — Excellent
- SIEM Engineering/Analysis

Proactive security expert ready to stand between businesses and threat actors. Lifelong student of developments in threat detection and mitigation. Adept at assisting with every stage of cybersecurity management, from preventive measures to disaster mitigation and recovery.

Work History

2021-03 - Current

Sr. SECURITY RESEARCHER

Zscaler

- Authored multiple companywide security policies, driving compliance and best practices into company culture.
- Developed and performed incident response protocols to mitigate damage and liability during security breaches and recover services within acceptable timeframes.
- Created cybersecurity best practice communications to educate staff and customers against known threats and potential vectors of attack.
- Spearheaded SOC overhaul, designed system architecture, engineered SIEM, EDR, SOAR, and data pipelines, crafted threat hunting workflows and engineered all security alerting automation.
- Integrated multiple intelligence sources to maximize threat hunting efforts.
- Guided company through FedRAMP authorization. Ensured 100% of requirements were met and led to FedRAMP High and Moderate authorization.
- Exceeded goals through effective task prioritization and great work ethic

2020-02 - 2021-03

INFRASTRUCTURE ENGINEER/SECURITY ENGINEER

NOVETTA

- Single-handedly designed security solution for 1500+ host network, operating at 15 remote sites, 6-month project to get NIST-800-171 & FedRAMP compliant from scratch.
- Developed SIEM and SOAR solutions for clients,

(ELK, Splunk)

Excellent

EDR Solutions (Crowd Strike, Elastic Agents, Custom Builds)

Excellent

Risk Mitigation/Management

Excellent

Operations Planning/Development (AGILE)

Excellent

including self-deploying environment for quick deployment/rebuilding built on Jenkins, Ansible, VMware Horizon/ESXi, python, and powershell.

- Software release management, including planning, installation, testing, troubleshooting, and risk acceptance/mitigation.
- AGILE/SAFe environment where customer satisfaction with product availability and usability were paramount.

2016-07 - Current

SR. SOC ANALYST, IR LEAD, SECURITY ENGINEER

USAF

- Currently in reserve status
- Applied leading theories and concepts of threat hunting to develop a MITRE ATT&CK oriented hunt plan unique to the customers risks and adversary priorities.
- Managed all SOC operations, including operations planning, incident response, threat hunting, vulnerability assessments, threat emulations, risk mitigation, designing SOC architecture, and engineering automation solutions.
- Drove network forensics using SIEMS such as ELK and Splunk and tools like Bro (Zeek), Snort (Suricata), and Moloch (Arkime) including engineering network traffic collection.
- Performed host forensics with tools like Endgame, Powershell, Sysmon, Volatility, Elastic beats/agents, and custom built tools to meet operational requirements.
- Planned complex missions to secure, investigate, and protect various unique DoD critical assets and networks.
- Managed teams of 20+ operators in their daily tasks and large project completion.

2012-01 - 2016-07

DATABASE ADMIN

USAF

- Administered, supported and monitored databases by proactively resolving database issues and maintaining servers for the largest payroll system on

earth.
- Designed and developed analytical data structures.
- 0 security incidents, 99.999% uptime.

Education

2021-01 - 2022-07

Master of Science: Cyber Security

Western Governors University - Salt Lake City, UT (Online)

2017-01 - 2019-06

Bachelor of Science: Information Technology Management

American Military University - Online

2016-01 - 2017-09

Associate of Science: Cyber Security

Community College of The Air Force - Montgomery, AL

Certifications

2019-08	Offensive Security Certified Professional (OSCP), Offensive Security
2020-01	Certified Information Systems Security Professional (CISSP), ISC2
2017-07	GIAC Certified Forensic Analyst (GCFA), GIAC
2021-03	Certified Ethical Hacker (CEH), EC-Council
2016-09	Security+ (SEC+), COMPTIA

Personal Projects

- Github
https://github.com/JasonBurnsInfosec/WOD_randomizer
This is a python project that demonstrates scraping arbitrary web data, parsing and transforming it, and finally application of the normalized data.
- Hackthebox
https://app.hackthebox.com/profile/overview
Ranked 489 globally