Chad Porter

Des Moines, IA
(515) 865-0880
chadaporter@gmail.com
chadporter.net
HackTheBox (Top 100): abselithat#11160
in/chadporterdev

SUMMARY

Experienced cyber security professional with a proven track record of developing and implementing effective security policies, tools, and processes to protect organizations. Adept and designing, testing, and supporting enterprise cyber security solutions.

EXPERIENCE

Senior Incident Response Analyst | Honda North America

August 2023 - Present, Marysville, OH

- Lead threat intel and incident response investigations with a team of analysts and reduced critical alert response times to 24 hours.
- Communicate complex threat insights through clear, actionable reports and presentations for leadership, stakeholders, and external partners.
- Manage an initiative to improve GRC risk analysis by adding security incident details, resulting in higher fidelity risk scoring.
- Directed 2 tabletop exercises to assess and refine incident response protocols, consistently raising coordination and preparedness across operational teams.
- Ensure SEC compliance by participating in assessments, aligning with industry standards, and recommending improvements to security protocols.

Senior Cyber Security Engineer III | Principal Financial Group

January 2020 - April 2023, Des Moines, IA

- Performed continuous operational support of QRADAR, Splunk, Crowdstrike, and Corelight Zeek/Suricata including architecture, policies, rule recommendations, tuning, and upgrades.
- Built 10+ high-fidelity incident detections based on threat actor analysis, attack methodologies, and intelligence sources.
- Performed artifact analysis of suspected threat actors using Crowdstrike Falcon Sandbox, completing 4 incident response investigations.
- Configured and maintained custom nTop NSM infrastructure on Debian Linux servers, maintaining a 99% uptime.
- Maintained and configured network monitoring tools, intrusion detection systems, web application firewalls, and data loss prevention tools.

SOC Analyst II | Pratum

September 2019 - January 2020, Ankeny, IA

- Performed event correlation and analyzed network traffic anomalies on security incidents in Fortinet SIEM appliances.
- Developed and executed 3 threat mitigation strategies, policies, and incident response procedures consistent with business strategies while effectively protecting data integrity, security, and limiting liability.
- Actively lead and triaged 5 incident investigations involving malware analysis from Microsoft Defender XDR driven alerts.
- Validated intrusion detection system (IDS) alerts against network traffic.
- Deployed infrastructure using Docker, Ansible, and Terraform on Linux systems and cloud-native services.

Information Security Analyst I | Pratum

September 2017 - September 2019, Ankeny, IA

- Analyzed and responded to security incidents from Fortinet SIEM appliances.
- Maintained and developed 100+ custom attack signatures on cyber defense network tools in response to analyzed threats.
- Analyzed requirements, risk analysis, and installation, and support of both physical and 20+ virtualized SIEM appliances.
- Increased efficiency of 10 critical alerts and reports through scripting automation.

PROJECTS

- gitlab.com/chadporter/custom-exploits
- gitlab.com/chadporter/winrm-shell | Improved WinRM shell using a custom DLL loader
- gitlab.com/chadporter/windows-exploit-writeup | Custom exploit and Defender XDR bypass technique using phantom evasion tool

EDUCATION

Management Information Systems | Iowa State University

Ames, IA, 2014

Information Technology Network Administration | Des Moines Area Community College

Boone, IA, 2011

CERTIFICATIONS

Certified Intrusion Analyst (GCIA) | **GIAC**
2018