Erik Cedillo

(415) 496-5068

therevolveruk@gmail.com

Skills

- **Elastic SIEM**
- **Microsoft Defender**
- **Crowdstrike Falcon**
- **Wireshark**
- **Snort**
- **Regex**
- **Yara**
- **Sigma**
- **MITRE ATT&CK**
- **Windows Internals**
- **Sysinternals**
- **Bloodhound**
- **Metasploit**
- **VirusTotal**
- **Wireshark**
- **NMap**
- **Palo Alto NGFW**
- **Fortinet FortiGate**
- **IBM Resilient SOAR**
- **Splunk SIEM**
- **Cuckoo Sandbox**

Certifications

Certified Information Systems Security Professional (CISSP)
ISC2
2019

GIAC Certified Incident Handler Certification (GCIH)
SANS
2021

Summary

SOC Analyst with five years of dedicated experience in security operations. Possesses a solid foundation in network protocols, malware identification, and forensic investigation, underpinned by a CISSP certification. Characterized by an exceptional ability to monitor, detect, and neutralize cyber threats. Proficiency in the latest SIEM technologies, coupled with a keen analytical mindset, allows for the adept handling of complex security incidents. The professional's expertise is further evidenced by a proven track record in enhancing SOC operational efficiency and reducing incident response times.

Experience

Sierra Nevada Corporation **10/12/20 – 3/10/24**
Security Operations Engineer Sparks, NV
https://www.sncorp.com/

- Perform real-time monitoring and triage of security alerts in SIEM and EDR
- Make accurate determination of what alerts are false positives or require further investigation and prioritization
- Lead and actively participate in the investigation, analysis, and resolution of cybersecurity incidents.
- Analyze attack patterns, determine the root cause, and recommend appropriate remediation measures
- Ensure accurate and detailed documentation of incident response activities
- Collaborate with knowledge management teams to maintain up-to-date incident response playbooks
- Collaborate with cross-functional teams, including forensics, threat intelligence and network administrators.
- Clearly communicate technical information and incident-related updates to management and stakeholders
- Monitor the performance of security analytics and automation processes

Nuance Communications **5/26/13 – 5/20/16**
Quality Assurance Specialist Cambridge, MA
https://www.nuance.com/

- Performed functional testing on voice-controlled virtual assistant app for mobile devices
- Capturing phone and server logs using Eclipse, adb (Android debug bridge), and custom software
- Logging bugs in Jira in accordance with defined standards, tracking them, and verifying fixes.
- Running automated tests on servers through basic XML coding, using predefined Python programs

Education

University of Texas San Antonio **2016-2020**
Cybersecurity Bachelors
3.96

SANS Institute **2020-2024**
Cybersecurity GIAC Certification

Website
https://revolveruk30.gitbook.io/