Gabriel Barrera

Information Security Analyst II

(619) 251-8136
gsbarrera1@gmail.com
San Diego, CA
github.com/GabeBarrera
linkedin.com/in/gbinfosec

Driven computer scientist skilled in problem-solving, software development, and building cloud solutions. Passionate about learning new emerging threats/techniques in cyber security, and implementing new and innovative mitigating controls and automations.

EDUCATION

Bachelors Science – Computer Science

San Diego State University
2015 – 2019

Relevant Courses

Cyber Security	Machine Learning
Systems Programming	Data Structures

TECHNICAL SKILLS

Languages
PowerShell, Python, JavaScript, PHP, KQL, SQL, Bash

Cloud Services
Microsoft Azure, Intune, O365, SolarWinds, Okta, Twilio

Tools
MS Defender XDR, Palo Alto, Power Automate, Power BI, Postman, Git, InfoBlox, Any.Run, VT, Rapid7, Ghidra

SOFT SKILLS

Verbal/Written Communication | Critical Thinking | Teamwork | Problem Solving | Adaptability | Self-Management | Design | Questioning

NOTABLE PROJECTS

The Hunt

- Implemented detection alerts, learned to read/write Russian, and investigated the chain of command to determine the legitimacy of a highly suspicious user.

The Sentinel Unified System (SUS)

- Integrated SolarWinds Service Desk, custom KQLs and Analytics Rules, Teams, and Logic Apps for a more efficient and robust security event detections and life-cycle management.

EXPERIENCE

Information Security Analyst → IS Analyst II

Port of San Diego
Nov 2019 – Present

- Reduced MTTD by ~70% and MTTR by ~30% by building a centralized event collection and alerting system in Azure cloud to serve as a stopgap solution until SIEM purchase and implementation.
- Leveraged Defender XDR, Azure Sentinel, Palo Alto traffic & InfoBlox queries to hunt for suspected or confirmed compromise, investigate and contain, and carry out remediation tasks while adhering to SLAs.
- Mitigated unauthorized access to sensitive machines and user accounts by implementing and maintaining Okta's MFA solution, configuring Certificate Based Authentication policies, regularly auditing IAM in Active Directory, and hardening OS per CIS benchmarks.
- Coordinated and advised LAPS and MFA server configuration efforts between IS and IT departments.
- Implemented App Registrations, Logic App flows, and PowerShell scripts that leveraged the Graph API to reduce time to audit and respond to security events as well as remediate general operational inefficiencies.
- Performed regular risk assessments of vulnerabilities found by Defender or Rapid 7, new apps created by IT, and SOC II / ISO27001 reports from third-party partners
- Analyzed suspicious EXEs with Ghidra and ClamAV.
- Developed KQL queries/rules for Defender and Sentinel to improve threat hunting/alerting based on research of emerging threats/risks and new critical vulns/IOCs.

Software Developer Intern

Port of San Diego
Jan 2018 – Nov 2019

- Aided recovery efforts of the Port of San Diego's Incident Response Team in restoring normal systems operations after a company-wide ransomware attack.
- Increased deployment efficiency and reduced workloads by crafting PowerShell and Python scripts to meet incident SLAs and software deliverable goals.