Vidur Ravella

ravella.vidur@gmail.com, +1-571-888-1327, www.linkedin.com/in/vidur-ravella

Technical Skills:

- *Network:* FireEye NX, Palo Alto Firewall, Splunk, RSA Netwitness, Wireshark, Arbor Cloud, Kibana, Bricata
- *Software Dev:* HTML, CSS, Java, MySQL, GitHub
- *Threat Intel:* Mandiant, Palo Alto Wildfire, Recorded Future
- *Endpoint:* FireEye HX/FX, Defender for Endpoint
- *Email:* Agari, FireEye EX, Ironport, O365
- *Vulnerability*: Verodin, Canary Tokens
- *Cloud:* AWS Guard Duty, Azure Security Center/Sentinel, Prisma, AWS GOV, GCP
- *Proxy:* Symantec Bluecoat, Fortiguard, Palo Alto
- *SIEM:* Helix, Arcsight, Splunk

Experience:

Optum |Senior Cybersecurity Analyst (SOC) *Jan 2020 – Present*

- Standardized training materials for 15+ full-time/rotational/intern employees and trained new hires
- Lead incident response processes to contain security-related incidents using NIST IR & MITRE ATT&CK framework
- Investigated hundreds of potential security threats and determined root cause through malware analysis and forensic analysis within AE/NIE and cloud instances
- Identified multiple security gaps during TTX/Purple Team Exercises and collaborated with CIRT teams to mitigate risk exposure to business
- Defined 70+ response playbooks for AWS Guard Duty and recommended security mitigations
- Performed in-depth tuning related analysis for SIEM and IDS/IPS rules
- Analyzed potential phishing emails using OSINT tools, sandboxes, and email headers
- Monitored network for thousands of IOC's collected through threat intel feeds and IDS/IPS rules using full packet captures(FPC), firewall, and proxy logs
- Engineered a formal monitoring intake process for the SOC to streamline workflow

Optum |Information Security Risk Analyst *June 2019 – Jan 2020*

- Approved security RITM's for EIS Customer Concierge Services (CCS)
- Published and automated metric reporting to evaluate the daily performance of various teams
- Developed a cybersecurity community outreach framework to increase employee engagement
- Collaborated with 50+ Acquired Entities to apply security controls during their M&A period
- Streamlined Plan of Action and Milestone Management (POAM) using Vulnerator for 3+ SISO's
- Engaged in vendor-led audits/TTX for 3 State Government contracts

Optum |IT Systems Management Intern *May 2018 – Aug 2018*

- Ensured a consistent method of incident management is adhered to
- Validated and verified 250+ Service Monitoring probe documents in adherence to business requirements

ITS Penn State |Lab Consultant Supervisor *Aug 2017 – May 2019*

- Maintained a thorough understanding of various software and machines in computer labs and classrooms
- Managed 110 Lab Consultants and encouraged efficiency in resolving incidents
- Diagnosed misconfigurations with printers, computers, and network-related devices

Education/Certifications:

- Pennsylvania State University *June 2015 – May 2019*
  - Bachelor of Science in Information and Cyber Security
- CompTIA Security+, MITRE ATT&CK SOC Assessments, Metro State Incident Handler, ServiceNow Fundamentals

Additional Skills: Risk Analysis, Data Analysis, Malware Analysis, SIEM Analysis, Threat Intel, IDS/IPS rule tuning, OSINT URL Analysis, Threat Hunting, TCP/IP Protocols, PCAP Analysis, Operating Systems

Active Interim T3 NAC Security Clearance