

Travis Trimboli

+1-240-676-1232 | travis.trimboli@gmail.com | [linkedin.com/in/travistrimboli/](https://www.linkedin.com/in/travistrimboli/) |

SUMMARY

Accomplished cybersecurity professional with over 8 years of experience helping organizations improve their operations across all security domains. Experienced in combining software and security engineering to support the development of threat intelligence programs and security operations. Passionate about threat hunting, detection engineering, and vulnerability management, using threat intelligence to drive proactive security measures.

Proven track record of leveraging technical and domain knowledge from education, certifications, and experience to deliver value to customers. continued learning, and hands-on experience to deliver strategic and technical expertise through all stages of program development. Skilled at providing creative, customer-centric, outcome-oriented solutions, and passionate about building collaboration between cross-functional teams and stakeholders to align vision with needs.

TECHNICAL SKILLS

Languages: Python, SQL, GraphQL, YAML, Bash, JavaScript

Development Tools: Atlassian (JIRA, Bitbucket, Confluence), Git, Ansible, Terraform, Postman, Kubernetes, Docker

Cloud Platforms: AWS, Azure, Google Cloud Platform

Data and Security: Splunk, Sentinel, Elastic, Pandas, Matplotlib, MITRE ATT&CK, Crowdstrike, STIX/TAXII

Management: Salesforce, Gainsight, ChurnZero, Pendo, Aha!

EXPERIENCE

- **CareFirst BlueCross Blue Shield** Baltimore, MD / Remote
Senior Cybersecurity Analyst - Threat Intelligence May 2025 – Present
 - Supported the development of the CareFirst Threat Intelligence Service program with tasks including:
 - * Advised smaller subsidiaries and clients on developing their security operations and threat intelligence programs.
 - * Adapted new tools and technologies to streamline processes and improve efficiency.
 - * Performed monitoring and analysis of threat intelligence data to identify trends and patterns.
 - * Produced actionable intelligence reports and briefings for stakeholders.
 - Managed threat intelligence operations, including threat hunting, detection engineering, and vulnerability management.
 - Actively participated in threat landscape and attack surface analysis to identify emerging threats and vulnerabilities.
 - Identified areas where threat intelligence can play an active role in improving organizational posture across multiple security domains from network and endpoint to the cloud.
 - Actively collaborated with security teams on threat intelligence program strategy including but not limited to:
 - * Establishing intelligence requirements.
 - * Creating useful workflows.
 - * Broadening cross-team collaboration.
 - * Executing on the creation, implementation, and integration of new tools and processes..
 - Developed custom tools including, a vulnerability prioritization system that uses various data points, including the NIST Likely Exploited Vulnerability (LEV) metric, and a threat actor analysis tool to analyze and visualize threat actor techniques, tactics, and procedures (TTPs).
- **ThreatQuotient** Reston, VA / Remote
Customer Success Engineer Feb 2019 – May 2025
 - Guided the development of the Customer Success program from the outset with tasks including:
 - * Advised in defining the Customer Success Engineer role and responsibilities.
 - * Helped determine the operational, tactical, and strategic approaches applied by the team.
 - * Introduced customer success metrics and KPIs and ways to track them.

* Adapted new tools and technologies to streamline processes and improve efficiency.

- Managed North American customers, including commercial, federal, and DoD, as a trusted advisor to SMBs and enterprise-level organizations comprising the Fortune 50, 100, and 500 lists.
- Advised stakeholders from the C-Suite to the primary contributor level on developing their security operations and threat intelligence programs.
- Identified areas where CTI can play an active role in improvising organizational posture across multiple security domains from network and endpoint to the cloud.
- Actively collaborated with security teams on CTI program strategy including but not limited to: establishing intelligence requirements, creating useful workflows, broadening cross-team collaboration, executing on the implementation and integration of new tools and processes, and taking full advantage of the platform to improve decision-making in critical situations.
- Contributed to custom integration and tool development to increase customer operational efficiencies.
- Delivered security program recommendations based on established frameworks such as MITRE ATT&CK, Palantir ADS, NIST CSF, and various compliance standards depending on industry.

- **Carbon Black**

Boulder, CO

Threat Analyst

Aug 2018 – Feb 2019

- Participated in a 24/7 SOC team working on rotating schedules.
- Performed endpoint security monitoring, security event triage, and incident response for a mid-size organization.
- Collaborated with other team members and management to document and report incidents to stakeholders.
- Maintained records of investigated security events and incident response activities utilizing case management and ticketing systems.
- Took on security operations responsibilities when not on active SOC shifts, including documentation, basic malware analysis, exceptions tracking, security tool management, tuning, configuration, and metrics and reporting.
- Contributed to the development of front-end applications to support SOC team operations.

Waltham, MA
Oct 2017 – Aug 2018

Sales Engineer

- Configured and presented product demonstrations for prospects, customers, and partners.
- Served as a client-facing technical resource supporting the sales organization.
- Completed product RFI/RFPs for all three products as they present themselves.
- Coordinated product evaluations and proof of concepts for prospects.
- Assisted product management with documenting usability and feature feedback.
- Supported prospect and customer implementations and continued success using the products.
- Provided internal support for any troubleshooting-related inquiries.
- Examined potential threats and provided analysis on how each product would respond.

• **Fidelis Cybersecurity**

Bethesda, MD

Account Manager

Feb 2016 – Oct 2017

- Conducted outbound and inbound B2B prospecting by phone and email for potential Commercial, Government, Defense, and Channel clients.
- Communicated core value propositions of Fidelis products and services to C-suite individuals of all industries.
- Qualified prospects based on needs, timelines, and budgets for the outside account team.
- Accelerated prospects through the sales cycle, promoting revenue-generating outcomes.
- Attended trade shows and partner functions to represent Fidelis, showcasing product components and gathering user feedback.

EDUCATION

• **University of Maryland Global Campus**

Adelphi, MD

Master of Science in Information Technology; GPA: 4.00

Aug 2017 – May 2020

• **University of Maryland**

College Park, MD

Bachelor of Arts; GPA: 3.80

Aug 2008 – May 2013

CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- AWS Certified Cloud Practitioner
- CompTIA Security+

PROJECTS

- **Vulnerability Evaluation System (VES):** Vulnerability prioritization system that uses various data points, including the NIST Likely Exploited Vulnerability (LEV) metric, to assess vulnerabilities and calculate a unique VES score.
- **TTP Analyzer:** Python application for parsing threat intelligence reports and analyzing MITRE ATT&CK Tactics, Techniques, and Procedures (TTPs) to understand threat actor evolution over time.