First Name Last Name

email@youtube.com
5555555555
Seattle, WA

Summary

Speak in 3rd Person.

Cody is a security professional, specializing in Vulnerability Management, Threat Modeling, Incident Response and Open Source Intelligence. Cody has worked for various Fortune 100 companies, reducing critical vulnerabilities to 0, reducing repetitive tasks through automation.

Cody is an organizer for his local DEFCON Group chapter, a YouTuber teaching Security and Open Source Intelligence.

Professional Skills

Qualys, Vulnerability Scanning, Vulnerability Prioritization , Incident Response, Project Management, OSINT, Threat Intelligence, Linux, Cyber Threat Intelligence, Windows Patching, Tenable, Program Management, CMMC, Policy Compliance Scanning, Executive Security, Bash Scripting, ChatGPT

Employment History

Cybersecurity Engineer

Employer 1 • Seattle, WA
04/2022 - Present

- Create documentation workflows for high visibility tasks (Vice President/CEO visibility).
- Plan working sprints on a weekly cadence.
- GovCloud/FedRAMP SME, investigating data discrepancies and resolving said discrepancies.
- Develop Athena queries for faster processing of metric information (host counts, vulnerability count, etc)
- Assist with customer engagement with "Vulnerability In The News" emails.
- Conduct vulnerability attack path simulations using the MITRE ATT&CK Framework
- Develop and automate AWS Athena queries

Youtube Content Creator

Self
03/2020 - Present

- Create content regarding OSINT (Open Source Intelligence)
- Assist Law Enforcement with locating Missing Persons and Criminals
- Manage business partnerships and sponsors
- Manage a Discord Community with over 800~ participants
- Mentor individuals from around the world, and purchased a PWK/OSCP class for one of my mentees

Organizer

DEFCON Group 253 • Tacoma, WA
08/2018 - Present

- Organize monthly meetings at Devils Reef Tacoma
- Community out reach via Social Media (Reddit and Twitter)
- Grown our community from 3 to over 100 since 2018
- Organize fundraisers and committees for Tacoma's first hackerspace
- Create dc253.org

Senior Cyber Security Engineer

Employer 2 • Tacoma, WA

11/2020 - 04/2022

- Onboard Employer 2 with the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploit List.
- Create automations for daily manual tasks (running and creating reports in Qualys) using the Qualys API.
- Work with partner teams streamline risk reduction through ticketing.
- Aggregate detections into a single report for stakeholders.

Vulnerability Management Engineer

Employer 3 • Herndon, Virginia
07/2020 - 11/2020

- Consult on Vulnerability Management Best Practices to include suggestions from NIST SP 800-151
- Coordinate 5-year scanning efforts with Employers's Business Units
- Plan 1 year and 5-year roadmap for Vulnerability Scanning and automation of remediation
- Work with Threat Intelligence team to prioritize Vulnerabilities
- Integrate scan data into Kibana for Patch Prioritization
- Automate border scanning using Shodan and Slack webhooks for alerting on risks outside of CVE's

Intelligence Consultant/Post-Sales Engineer

Employer 4 • Seattle, WA
03/2020 - 05/2020
Provide training to clients of the Recorded Future platform, find upsell opportunities and work with internal teams to find new opportunities. Provide context on threat intelligence research with IOCs, threat actors, ongoing cyberattacks, and geopolitical events.

Cyber Security Engineer

Employer • Seattle, Washington
05/2014 - 05/2020

- Provide Vulnerability Management and Threat Intelligence training to members of the Gov Agency as well as the Gov Agency.
- Participate in Capture-the-Flag events to include event This event was a multinational/multiservice event. Our team ended up winning
- Threat Intelligence SME and provide monthly updates to the unit on the newest vulnerabilities
- Provide hands-on training with tool and tool.

Cyber Security Consultant

Mark V Security • Tacoma, Washington
08/2018 - 03/2020

- Conduct Penetration Tests for clients to include Network Scans, Exploiting Vulnerabilities, Account Pivoting.
- Consume Gigabytes of text data and filter down results with Linux commands such as grep, sed, and awk.
- Write Post Engagement reports to include Executive Summaries and Technical Details about the engagement.
- Assist clients with Post-Engagement follow-ups to include implementation of guidance provided by Consultants.
- Develop a breach calculator on the Mark V Security website (https://markvsecurity.com/invest.html).

In this role, Cody has worked with Mark V Security to perform Penetration Testing, Vulnerability Management, and Security Assessing. Various red-team tools in this position were used to perform testing, such as Bloodhound, Metasploit, Responder, EyeWitness, etc. Cody's testing was translated into reports, which included an Executive Summary, Findings, Technical Details, and Recommendations.

This position allowed Cody to work with various organizations to mature their security programs.

Vulnerability Management Analyst

Employer • Seattle, Washington
11/2015 - 03/2020

- Provide in-depth analysis of threats to company's corporate infrastructure
- Lead Vulnerability Scanning projects against ICS, Network Infrastructure, and Subsidiaries
- Work with external researchers on vulnerabilities found on site.com, which lead to the site VRP (Vulnerability Reporting Program) that is active on HackerOne

Reporting Program) that is active on HackerOne.
- Work with Legal, PR, and Incident Response teams to report vulnerabilities found on Open Source Software.
- Lead proactive threat and vulnerability scanning efforts utilizing Open Source feeds such as Social Media, News Outlets, and other forms
- Onboard company Subsidiaries to remote authenticated scanning as well as agent-based scanning
- Microsoft Patch Tuesday SME and orchestrating meetings with development teams and corporate system teams.

As a Vulnerability Analyst, Cody was able to streamline a few processes that needed updating. One project Cody immediately took ownership of was the use of Third-Party software tracking. Cody was able to streamline the manual process by working with our Automation Team to ingest products and versions using the Vendors API. This process was then changed to a self-service program that cut back time and costs associated with Software Tracking. Cody also leads the change of adding Threat Intelligence to the scoring and prioritization of Vulnerabilities by revising the corporate-wide Patching Policy to include CVSS scoring and Threat Intelligence scoring.

Education

SEC401: Security Essentials Bootcamp Style

SANS • San Diego, California
05/2017

SEC560: Network Penetration Testing and Ethical Hacking

SANS • New York, New York
08/2018
SEC560 covered network penetration testing fundementals to include Network Scanning, Exploitation, Password Attacks, Pivoting and Web App Pentesting. This course provided 37 CPE's.

SEC487: Open-Source Intelligence (OSINT) Gathering

SANS • San Diego, California
05/2019
SEC487 covered the basics of Open Source Intelligence gathering and analysis to include finding intelligence on social media, geospatial, imagery, networks, governments and dark web. This course provided 36 CPE's. The exam for this course is pending Public Release in August 2020.