Jonathan K. Todd

Augusta, GA USA | 318-663-2982 | jonathan@valhall.ai | www.linkedin.com/in/jonathanktodd

Summary

I'm a highly self-driven cybersecurity professional, software engineer, and AI researcher searching for an innovative company to solve hard problems with.

Last year I built a following of 7,494 professionals in ~12 months by researching, exploring, experimenting with, and finally writing about my favorite topics. I love diving deep into granular technical details such as this publication which discusses threat detection down at the Assembly code level. However, some of the work I'm most proud of includes my soft-skill focused writings such as this one, published by CISO Robert Wood.

Automation + AI Newsletter (2,367 subscribers) [Introduction]

- ChatAPT [BSides Presentation], [Outline]
- Successfully Mitigating LLM Bias: Introspection & Prompt Engineering with my open source project LLM-Genie!
- The Prompt Injection Mitigation Problem is Never Going Away.
- Prompt Engineering & Context Framing: Taking Large Language Models to the Next Level
- Valhall.ai / Prompt Injection Mitigations
- Bringing AGI to the SOC. What, Exactly, is the Value Proposition?
- Tool Devs: You Should "Roll Your Own" Neural Network (Once)
- Hacking With GPT-4: Generating Obfuscated Bash Commands

Endpoint Threat Detection (& Evasion)

- I attempted to diagram everything I've learned about the problem-set of endpoint threat recognition over the past 2 years of research.

Mentoring

- After living and breathing cybersec for the past 3 years, here are the best resources I've found.

Soft Skills

- Metacognition: 'Thinking About the Thinking' is the Key to Professional Success
- Understanding How You Can Be Valuable In Cybersecurity Without Experience: Proven Potential
- A new era of FAR cheaper cybersecurity and IT is here! And no one cares.
- Pile-On Cybersecurity & Our Conflict of Interests
- Understanding VS Wisdom in Cybersecurity: 🌊 A Deep Dive
- Writing is the #1 Cybersecurity Skill. Here's Why Education Probably Didn't Prepare You For It.
- The Cybersecurity Problem-Set, Modeled.

Supply Chain Security

- Maybe We're Doing This Software Supply Chain Security Thing Backwards.

Compliance

- Self-Attestation for Government Contracted Software Supply Chain Providers: 🤕

Misc

- Cons of the Sec+ Certification

And finally, a value emphasized in my cybersecurity writings that I think is the most valuable trait to have in this profession:

Be curious, love the challenge:

> “None of this should feel like a chore, or some overwhelming mountain to climb. You should be like an astronomer looking up at the sky and realizing how little you know, and not be stressed by that, but rather excited and curious to uncover its mysteries.”

Relevant Experience

Computer Repair & Malware Removal Technician, A&G Computer Services (Natchitoches LA) | Part Time

- I removed malware from computers and replaced damaged hardware components.
- Preserved / restored lost data when possible.
- Set up home automation software.
- Was required complete repair tasks to meet deadlines.

Tier II Remote Tech Support Agent, Comcast | Full Time | ~2017 - October 2018.

- I worked with a ticketing system and fairly advanced sensor data from the routers to diagnose the customer’s problem (and usually solve it).
- I gained experience with time management and meeting strict productivity metrics.
- I overcame communication and access challenges of working remotely.

Cryptologic Network Warfare Specialist (Trainee), U.S. Army (Joint Cyber Analysis Course) | Full Time | February 2019 - May 2019

- I learned a number of cybersecurity related subjects through practical & knowledge-based exams over a 6 month 2000 hour course.
- Operating Systems (Windows, Ret Hat Linux, Solaris)
- Programming & Scripting Languages (Python, C++, Bash, PowerShell)
- Exploit Development
- Malware Analysis
- Digital Forensics
- Traffic Analysis

- Network Protocols
- Active Directory

Cryptologic Network Warfare Specialist / Computer Network Defense Analyst, U.S. Army & National Security Agency | Full Time | May 2019 - May 2021

- I analyzed network traffic. I have to be purposely vague due to the nature of the work.
- Started a tool development initiative (data visualization) to improve a capability.
- This was a very teamwork oriented role, as most military job roles are.

Cyber Operations Specialist (Trainee), U.S. Army | Full Time | May 2021 - January 2022

- Expanded upon and revisited the knowledge learned at JCAC in a format more focused on practical, hands-on CTF format.
- Operating Systems (Windows, Linux)
- Programming & Scripting Languages (Python, Bash, PowerShell)
- Exploit Development
- Malware Analysis
- Digital Forensics
- Traffic Analysis
- Network Protocols
- Active Directory

Cyber Operations Specialist, U.S. Army | Full Time | January 2022 - Present

I currently work as a host analyst on an ICS focused Cyber Protection Team within the Cyber Protection Brigade. I perform a threat hunting and incident response role, with a focus on analysis of Windows event logs through Elastic Search. I constantly innovate, propose more scalable and robust solutions to key technical challenges, and regularly encourage my organization to evolve toward better threat hunting methodologies and processes. I also leverage my skills as a software engineer to interface with big data APIs to take advantage of data science and automation toward the goal of improved threat detection capabilities.

I'm looking forward to transitioning to the private sector, where I hope to get involved with a team more open to cutting edge, innovative approaches to cybersecurity challenges.

References

Contact info available upon request.

Robert Wood, CISO @ Centers for Medicare & Medicaid Services - I agreed to write an article on soft skills in cybersecurity to be published by his project, Soft Side of Cyber.

Chris Hughes, President @ Aquia | Cyber Innovation Fellow @ CISA | Chief Security Advisor @ Endor Labs, and one of my hero thought leaders.

Jonathan Loop, CEO @ Harpe Engineering - I provided his company with technical consulting on AI engineering goals within a government contract.

Matthew Jay, Partner & COO, Cyber & Risk Management @ PC Techware - I met with him to discuss his interest in a security posture shift toward secure-by-design operating systems that I had written about, and this promising model's market viability for MSPs and MSSPs.

Walter Haydock, CEO @ StackAware - A Harvard MBA, long time mentor, and leading policy and risk management expert of AI & cybersecurity on LinkedIn, with a following of 13,982.

Captain Kuhn @ US Army - A great and caring leader currently supporting my efforts to propose and enact much needed reforms.

Chief Warrant Officer Smith @ US Army - A leader and subject matter expert on my current Cyber Protection Team.

First Sergeant Smith @ US Army - The best senior leader and mentor I met during my service.

Staff Sergeant Alibrahim @ US Army - A senior supervisor, mentor, and wise leader.

Staff Sergeant Morrell @ US Army - A recent supervisor and highly supportive leader.

Sergeant Frazier @ US Army - A supervisor I served with on a ceremonial detail to bury & honor our dead.

Sergeant Le @ US Army - My current direct supervisor and a skilled endpoint analyst.

Sergeant Keely @ US Army - My former direct supervisor and one of the most patient and professional leaders I've had the pleasure of serving with.

Certs

- Sec+

I have nothing against certs, but I personally rather invest my free time coding my own software, performing my own research projects, developing presentations for my leadership to improve internal processes, watching informative videos, and engineering / tinkering with cloud, infrastructure as code, data science and other fun challenges instead!

Relevant Projects

Chat-APT

An AI research project I presented at BSides Augusta to an audience of hundreds. A cybersecurity red-teaming framework which demonstrates the emerging threat possible by leveraging Large Language Models (LLMs) such as GPT to elevate high-fidelity social engineering effort to an unlimited scale.

LLM-Genie

This is a TypeScript (for front-end and Node.js) project serving as middleware for LLM API usage to add robust features such as:

- Bias mitigation
- Boolean selection
- Summarization
- List generation
- Choice selection
- And soon to include Remotely Augmented Generation (RAG), plus much much more.

See: [article] [playground] [repository]

Stack Hunter

This acts as a framework gluing together and integrating 4 existing technologies/resources toward the goal of streamlining threat hunting training and detection engineering:

- Caldera (a MITRE-developed threat emulation framework)
- Jupyter (a note-book computing apparatus which excels with data-science and rapid GUI prototyping)
- Kubernetes / Terraform (infrastructure configuration)
- ELK (Elastic Search)
- MITRE ATT&CK Framework (taxonomy / threat intelligence)

This project involves spinning up an active directory environment, running a threat simulation, recording the resulting security and network logs in ELK, and facilitating both developer and non-developer analysts on the team to hunt leveraging custom-made threat hunting analytics facilitated by the tool. Validation of these analytics through the analysts’ threat hunting success is then automated.

I paused this project’s development when GPT-3 was released, after which I transitioned to an AI focus, a decade long passion of mine.

Endpoint Threat Detection Methodology Research

I spent years captivated with the challenge of identifying state-of-the-art obfuscation in x86-64 machine code. After a year of brainstorming with a malware analyst colleague on this topic, I put a rather ambitious approach to the problem on paper in the form of a ~50 page report. I proposed to analyze many small chunks of code, just-in-time ahead of the instruction pointer via a form of black-box-analysis to match any two known-bad obfuscated code samples without needing access to the attacker’s source code. I began developing a GPU compute shader in an attempt to write an x86-64 fetch, decode, execute cycle that could execute millions of times in parallel to make this computationally expensive process feasible in real-time. Upon peer review, my approach was determined to be mathematically infeasible. But I continued the research through alternative approaches.

Three-Part Endpoint Defense Research

(PDF) After my previous paper, I was still interested in pursuing this problem-set. This time I proposed the Monte Carlo tree search, in place of my prior more brute-force approach. And this time, in order to prevent a kernel-level attacker from over-writing / disabling the defense system, I proposed a modified DDRM technology which externally injects the scanning program into a truly random location in memory and executes that code via JTAG. A hardware based solution is also proposed to allow the effectiveness of cold-storage without the need for a physically separate drive.

Cybersecurity Community Activism

My Reddit account (https://www.reddit.com/user/Jonathan-Todd) documents my history of frequent discussion and publication of cyber security concepts, technologies, questions, and research. My activity is exclusively Cybersecurity focused, so my entire post and comment history should serve as validation. This activism has benefited me greatly through observing the countless practical, “gray area” details of the cybersecurity industry not learned through certifications, courses, nor military service.

Personal Development

Self Education

My life is YouTube cyber security self-education and coding. I have watched every video in this 268 video YouTube playlist (I add every interesting video I find to watch or re-watch later) and many more. I am also beginning to work toward acquiring certifications.

Software Engineering Hobby

I love automation and tooling via software engineering. I have a decade of coding experience including the following languages (in order of experience level): JavaScript / Node.js, Python, HTML, CSS, PowerShell, PHP, and entry level tinkering with Bash, C++, and Assembly. I code for fun, but have studied professional processes such as Agile, DevSecOps, CI/CD, version control, and documentation best practices.