Justin M. Wray

Information Security Leader

An Information Security Leader with over two decades of experience helping clients secure their organization. With expertise across industries and technologies, Justin assists clients with assessing, designing, and implementing secure solutions, policies, and processes.

 York, PA

 wray.justin@gmail.com

 linkedin.com/in/justinwray

 justinwray.com

 (717) 916-5066

 github.com/wrayjustin

SUMMARY

A career dedicated to helping organizations navigate the complexities of data, technologies, and information security. Vast experience spanning from start-ups to Fortune 100 companies, non-profits to government entities, and across verticals. Worked with a wide range of technologies, from the network to the cloud, from the application to the data.

A passion that extends beyond the technology, focusing holistically on assisting organizations with securing their future.

- Executive leadership experience for cybersecurity organizations and a startup
- Managed in-person and geographically dispersed teams
- Telecommuted and worked from home office for over a decade
- Extensive experience in network security implementation and management
- Lead of penetration tests, vulnerability assessments, and red team engagements
- Have discovered, researched, and disclosed numerous vulnerabilities in both networking appliances and operating systems/applications services
- Long-term programming experience with multiple interpreted and compiled languages
- Experienced in both proprietary and open source applications - participating in the development of many open source applications
- Have designed, developed, maintained, and deployed web applications and services, working on both backend and front-end components
- Have provided network, hardware, and systems installation and support
- Managed many projects in professional capacities, educational settings, and freelance operations
- Team Lead for countless technical teams and projects
- Provided training in academic settings as well as practical training for professionals
- Developed course curriculum, training materials, and cyber exercises

---

ACHIEVEMENTS

- Discovered, disclosed, and reported numerous security vulnerabilities
- Discovered multiple undisclosed vulnerabilities
- Involved in development of multiple proprietary and open source projects
- Contributed to information security curriculum for colleges
- Participate in improvement of CyberWatch (a collaboration between multiple two-and-four year colleges to standardize information security coursework, degrees, and certifications)
- Developed information security labs, lectures, and curriculum for two-and-four year colleges and universities
- Served as a guest lecturer in many college-level information security courses
- Spoken at numerous conferences and cybersecurity events
- Presented numerous speeches to the likes of the National Science Foundation and the Military Cyber Security Conference
- Participate in both offensive and defensive teams in cyber exercises and competitions
- Competed and won countless individual and team-based cybersecurity competitions and exercises
- Designed, developed, and hosted a vast number of public and private cybersecurity competitions and exercises
- Created challenges and content for collegiate, commercial, government, military, and private cyber exercises

SKILLS & FOCUS AREAS

- Leadership
- Security Advisory
- Technical Assessments
- Governance, Risk, and Compliance
- Incident Response
- Application Security
- Cloud Security
- Security Solutions
- Application Development
- Information Technology
- Security Tools

EXPERIENCE

Director; Security Advisory Services NRI *February 2019 - Present*

Provide leadership of the Security Advisory Services division of a business technology consulting organization. Lead innovation, strategy, and vision for internally delivered offerings and engage in sales and marketing. Focused on security advisory, guidance, consultation, governance, compliance, risk management, assessments, and incident response. Provide oversight and direction for external client engagements as well as internal security programs.

- Provide leadership for global cyber security practice
- Manage delivery teams for cyber security products, services, and consulting
- Growing the security team by more than three times
- Increasing revenue and profit, year over year, over four times
- Lead technical and compliance security assessments
- Coordinate large-scale international incident response engagements
- Conduct and assist with pre-sales, marketing, and opportunity closing

---

Founder & Chief Executive Officer WraySec *September 2015 - February 2019*

Founded and managed a start-up focused on high-fidelity cyber training and security consulting. Managed day-to-day operations and client engagements for various services, including security assessments and application development. Led internal development efforts for proprietary security solutions, focused on cyber range design, deployment, and management, as well as a cyber exercise platform.

- Led geographically dispersed Cyber Security startup
- Provided executive leadership and company vision
- Engaged with clients for product and service scoping and delivery
- Coordinated with internal teams for project execution

Technical Specialist; Cloud & Offensive Security ICF International *February 2016 - September 2017*

Managed classified research projects for a confidential military organization (U.S.) in the areas of cloud security and offensive cyber warfare. Managed project teams of researchers and developers on both mission-oriented and fundamental research projects. Developed security tools, mechanisms, and capabilities for both offensive and defense cyber operations.

- Provided offensive security expertise
- Managed project teams of engineers and developers
- Directed project planning, tasking, and management
- Coordinated across multiple teams and organizations
- Engineered cybersecurity, tools, and mechanisms
- Developed training curriculum for new hires
- Coordinated and trained new hires

Manager; Penetration Testing Axxum Technologies *May 2015 - February 2016*

Managed an internal Red Team for a confidential federal government (U.S.) organization. Led penetration testing and vulnerability management programs. Developed security programs, policies, procedures, and documentation. Collaborated with executive leadership on security posture improvements and coordinated with IT teams to facilitate risk remediation. Designed, coordinated, and delivered security-related training across the organization.

- Managed a remote penetration testing and vulnerability assessment team
- Directed project planning, tasking, and management
- Coordinated with clients for engagement scoping and delivery
- Developed internal security policies and procedures
- Liaised with internal teams for vulnerability management
- Delivered weekly and monthly reports and briefings for executive leadership
- Performed threat emulation during assessments (red team)
- Developed training curriculum for new hires
- Coordinated and trained new hires

Engagement Lead & Researcher; Cyber Exercises iSight Partners *October 2012 - May 2015*

Designed, managed, and delivered large-scale cyber exercises for public and private training and competitive events. Leveraged threat intelligence and research to architect realistic scenarios for cyber warfare operators and industry professionals. Integrated real-world technologies and client configurations into cyber ranges for high-fidelity simulated events and training.

Cyber Exercise Engagement Lead *January 2014 - May 2015*

- Led cyber exercise and training engagements
- Engaged potential clients and solicited sales
- Managed customer delivery team of approximately seven individuals
- Coordinated with clients for exercise planning and delivery
- Planned and created cyber exercise training and scenarios
- Delivered exercises to cyber warfare operators and industry professionals
- Integrated real-world products and technologies into exercise environments
- Performed adversarial activity during engagements (red team)

Cyber Exercise Engineer and Researcher *October 2012 - January 2014*

- Engineered cyber warfare simulation platforms and environments
- Planned and created cyber exercise training and scenarios
- Delivered exercises to cyber warfare operators and industry professionals
- Coordinated with clients for exercise planning
- Integrated real-world products into exercise environments
- Participated in cyber warfare exercises and games
- Researched current cybersecurity threats and technologies
- Developed offensive automation tools and frameworks
- Maintained, updated, and deployed large code bases
- Tested and audited current and new projects
- Performed system and network administration

Network Security Analyst and Researcher ICF International *October 2007 - October 2012*

Managed global real-time threat detection and analysis infrastructure and tools. Led analytical processes, development teams, and research projects focused on cutting-edge threat intelligence and hunting.

Network Security Engineer and Researcher *March 2009 - October 2012*

- Managed project teams of engineers and developers
- Developed cutting-edge computer network defense infrastructure and tools
- Directed project planning, tasking, and management
- Researched new projects
- Tested new tools and methodologies
- Developed intrusion detection systems, tools, and mechanisms
- Planned and created security solutions
- Tested and audited current and new projects
- Maintained, updated, and deployed large code bases
- Integrated solutions into large production environments
- Engineered network security plans and goals
- Developed training curriculum for new hires
- Coordinated and trained new hires

Senior Network Security Analyst *October 2007 - March 2009*

- Real-time analysis of network traffic to detect intrusions and vulnerabilities
- Coordinated network incident handling with sites worldwide
- Managed and developed intrusion detection system signature and rule sets
- Released situation awareness reports
- Developed intrusion detection systems, tools, and mechanisms
- Tested new tools and methodologies
- Advised clients of security risks
- Engineered network security plans and goals
- Developed training curriculum for new hires
- Coordinated and trained new hires

Level II- IT Support Technician Constellation Energy Group *August 2006 - October 2007*

Provided advanced technical support services for regional, national, and global divisions in the energy sector. Through cross-functional liaison activities, delivered technical subject matter expertise, focused on networking and security.

- Provided level II technical support
- Reviewed large-scale technical issues
- Liaison between multiple departments and support center
- Developed and maintained new hire training schedule and information
- Managed technical projects and supporting teams
- Created support tools
- Authored documentation of knowledge bases and training materials
- Maintained knowledge bases used within support center and multiple support units

---

Network & Security Administrator / Supervisor HI–Tech Processing Services *August 2005 - August 2006*

Designed and managed the technical infrastructure, including network and security administration, for a data digitalization company. Provided technical leadership and expertise for a technical support and repair division focused on both commercial and consumer technical services.

- Managed public PC repair shop
- Developed processes for new projects and work
- Serviced and supported internal computers, printers, and phones
- Secured internal computers, printers, and telecommunication systems
- Evaluated technologies for implementation throughout the organization
- Created and maintained multiple databases
- Designed and developed Intranet site for corporate communications
- Managed multiple production and public web servers
- Monitored multiple production and DMZ servers – as well as Firewalls and Network Intrusion Prevention Systems

---

ADDITIONAL EXPERIENCE

Freelance / Consulting *June 2002 –Present*

Providing a wide spectrum of information security services to clients, including the assessment, design, and implementation of secure solutions, policies, and processes.

- Implemented and designed security solutions
- Tested and audited client environments
- Performed incident response and continued security monitoring
- Designed, supported, and maintained computer and network infrastructure

---

Warrant Officer; Cybersecurity Unit Maryland Defense Force *May 2013 - May 2017*

Served as a Warrant Officer in the Maryland Defense Force (Maryland State Guard), a military division of the Maryland Military Department. Assigned to the Cybersecurity Unit focused on providing cybersecurity services to the State of Maryland, as well as augmenting other military divisions.

- Performed Vulnerability Assessments and Penetration Testing
- Provided Cyber Security Training
- Supported Maryland: Defense Force, Army National Guard, and Air National Guard

---

Adjunct Professor; Cybersecurity Community College of Baltimore County *August 2010 – January 2015*

Founded and managed a start-up focused on high-fidelity cyber training and security consulting. Managed day-to-day operations and client engagements for various services, including security assessments and application development. Led internal development efforts for proprietary security solutions, focused on cyber range design, deployment, and management, as well as a cyber exercise platform.

- Taught multiple information security and networking classes
- Developed lesson plans and exams
- Delivered class lectures
- Administered class laboratory exercises
- Designed semester projects focusing on real-world applications
- Supported, motivated, and assisted students

PROJECTS

Notable or Public Projects

YAIDS *https://yaids.io/*

YAIDS is a Multi-Threaded Intrusion Detection System using Yara. YAIDS supports all valid Yara rules (including modules) and any PCAP-compatible data stream (Network, USB, Bluetooth, etc.).

ChatCTF *http://chatctf.com/*

ChatCTF is an interactive AI Chatbot designed to assist users with solving or creating capture-the-flag (CTF) challenges. However, devised as an Offensive and Defense Cybersecurity expert, ChatCTF additionally provides a new method for obtaining cybersecurity-related advice and assistance. ChatCTF is built upon OpenAI ChatGPT (GPTs), thus providing a familiar interface and interaction for users.

TeamSploit *https://teamsploit.com/*

TeamSploit makes group-based penetration testing fun and easy, providing real-time collaboration and automation. TeamSploit is a suite of tools for the Metasploit Framework. TeamSploit should work with any MSF product (including Community/OpenSource, Express, or Pro).

DTFTB *https://github.com/wrayjustin/dtftb*

Defensive Tools For The Brave (DTFTB) is a collection of Windows and Linux tools that automate: post-exploitation, backdoor, and rogue access discovery, for defenders. DTFTB allows a system defender to quickly and precisely locate common backdoor tendencies and system misconfigurations used by attackers to maintain access.

Unsploitable *https://github.com/wrayjustin/unsploitable*

Unsploitable is an emergency patcher, providing critical security patches and updates for commonly exploited vulnerabilities in common operating systems, services, and applications.

NetProfiler Suite *https://github.com/wrayjustin/netprofilersuite*

Automatically profile your network, building a packet filter of common known-good traffic. Useful for IDS filtering and network monitoring.

PhishingBoat

An automated Phishing Simulation and Assessment deployment platform that combines numerous phishing platforms and capabilities (such as GoPhish, Evilginx, etc.). Provides the ability to send phishing emails, harvest credentials and tokens, and deliver customized per-user payloads, all while providing robust reporting metrics.

---

sCOREcard (NRI)

An interactive web application for security engagement reporting platform. Allows for tracking, trending, sorting, and searching complex security data across initiative types (from technical assessments to physical security and social engineering to compliance reporting).

Facebook CTF Platform (FBCTF) *https://github.com/facebookarchive/fbctf*

The Facebook CTF is a platform to host Jeopardy and King of the Hill style Capture the Flag competitions. Owned by Facebook and used both internally and for numerous public-facing Capture The Flag events.

Cyber Exercise Engine (WraySec)

A comprehensive cyber exercise, training, and competition platform. Providing real-time event scoring, interactive range and scenario development, and a fully web-based experience for participants. Scoring includes service-based, task-based, and question-based, all available in mix-modes and individually or team-based.

ThreatSpace (iSight Partners; Mandiant) *https://www.mandiant.com/academy/threatspace*

A cyber exercise/competition platform and range for network attack, defense training, and simulation. Providing round-based service scoring or question-based scoring for team-based events.

Next Generation IDS (ICF)

A next-generation intrusion detection engine with a focus on speed, efficiency, advanced pattern matching, parallel processing, modularity, and expandability. Based on Regular Expressions, the IDS provides the means to write rules for malicious indicators and anomalous traffic in a singular mode.

Cyber Warfare Games

Develop and Deliver Capture the Flag (CTF), Red versus Blue (RvB), and King of the Hill (KotH), cyber warfare events.

Cyber Exercise Scenarios and Targets

Design and development of high-fidelity, real-world-based cyber threat scenarios for training exercises (cyber exercises, simulations, and tabletop exercises). The development of real-world analogous targets for private (isolated) range interaction, including platforms such as Google, Facebook, Twitter, Reddit, Amazon, eBay, etc.

OpenSearchEx

A search engine and web crawler using natural language processing for search engine functionality within an isolated cyber range. Designed to provide an analogous approximation of the Google search engine while providing critical search capabilities within a range. Implements a “PageRank” style algorithm to provide result relevancy for content discovery in an isolated/private environment. Although designed as a cyber range/exercise scenario asset, it can also be used for search capabilities within other offline environments.

---

tinc-sdwan

A zero-trust SDWAN solution, providing mesh networking through a software-defined wide area network. tinc-sdwan extends the tinc VPN client to provide zero-config SDWAN capabilities, allowing clients to communicate natively regardless of physical network location (remotely) or network filtering.

---

metashell *http://sourceforge.net/projects/metashell/*

metashell is a lightweight, heavy punch, interactive, intelligent command-line shell. The amazing difference with metashell lies in its ability to determine a file's datatype and automatically run your desired applications

---

twitter2rss

twitter2rss will obtain all friends of a specified Twitter account and then create an OPML feed list. The feed list will contain all of the obtained friend's Twitter RSS feeds, which can then be imported into any standard feed reader.

SpeedRead *https://wrayjustin.github.io/SpeedRead/*

SpeedRead is a featureful web-based, gamified, sight word learning program. SpeedRead is based on the "Dolch" Sight Word list and provides default words based on the target education level.

ADDITIONAL PROJECTS & CONTRIBUTIONS

- Kali Linux
- BackTrack
- Snort
- NMAP
- PBNJ
- Lak-IPS
- Bluesnipe
- Grav CMS
- Ubuntu Linux
- CoSign Coin

SKILLS

- **Leadership**
  - Strategy & Vision
  - Team Management
  - Project Management
  - Hiring & Training
  - Client Engagement
  - Sales & Marketing
  - Finance, Budgets, And Accounting
  - Security Advisory (Guidance And Consultation)
- **Technical Assessments**
  - Red Team Engagements
  - Penetration Testing
  - Social Engineering Engagements
  - Physical Security Assessments
  - Cloud Security Assessments
  - Vulnerability Management
- **Governance, Risk, And Compliance**
  - Policy And Procedure Evaluation
  - Policy And Procedure Development
  - Strategy Development
  - Compliance Audits And Assessments
- **Incident Response**
  - Planning And Readiness
  - Emergency Response
  - Incident Investigation
  - Incident Recovery And Remediation
  - Training And Exercises
- **Application Security**
  - Secure Coding
  - Dynamic Application Security Assessments (DAST)
  - Static Application Security Assessments (SAST)
  - Web Application Assessments
  - Mobile Application Assessments
  - Development Security Operations (DevSecOps)
- **Cloud Security**
  - Amazon Web Services (Aws)
  - Microsoft Azure
  - Google Workspaces And Cloud
  - Openstack
  - Containerization, Virtualization
  - Cloud Security Operations (CloudSecOps)
- **Security Solutions**
  - Intrusion Detection/Prevention
  - Firewall And Network Access Control
  - Anti-Malware And Endpoint Detection And Response
  - Monitoring And Logging
- **Application Development**
  - HTML, CSS, And JavaScript
  - PHP
  - C/C++
  - Perl
  - Python
  - Ruby
  - Go, Rust, Wasm
  - Source Code Versioning (Svn, Git, Etc.)
  - Package Development (Deb, Rpm, Etc.)
  - Continuous Integration / Delivery (CI/CD, DevOps)
- **Additional Technologies**
  - Mysql, Postgresql, And Sqlite
  - Bootstrap And Jquery
  - Linux Administration
  - Windows Administration
  - Apple Macos Administration
  - Hypervisor Administration (VMWare, KVM, Etc.)
  - Containerization (Docker, Kubernetes, Lxc)
- **Security Tools**
  - Kali Linux
  - Nmap / Zenmap
  - Snort, Yaids, Suricata, And Zeek
  - Nessus, Qualys, And OpenVAS
  - Metasploit
  - Gophish, FiercePhish, And EvilGinx
- **Soft Skills**
  - Verbal & Written Communication
  - Problem-Solving
  - Efficiency And Automation
  - Document Tools (Microsoft Office, Etc.)
  - Creativity

ACCOLADES

- **One Core Award** (Employee Recognition); NRI; 2020
- **One Core Award** (Employee Recognition); NRI; 2019
- **Exercise Lead** and Challenge Creator; USITCC-SC; 2018
- **Exercise Lead** and Challenge Creator; Cyber Spark; 2018
- **Exercise Lead** and Challenge Creator; MDC3; 2017
- **Exercise Lead** and Challenge Creator; USITCC-SC; 2017
- **Technical Lead**; MD National Guard Cyber Defense Team; 2017
- **Exercise Lead** and Challenge Creator; USITCC-SC; 2016
- **Technical Lead**; MD National Guard Cyber Defense Team; 2016
- **Technical Lead**; MD National Guard Cyber Defense Team; 2015
- **10 Years Participation** Award; MA CCDC; 2015
- **Gold Team** and Exercise Operations; MA CCDC; 2015
- **Challenge Creator** and Operations; NCL; 2015
- **Technical Lead**; MD National Guard Cyber Defense Team; 2014
- **Gold Team** and Exercise Operations; MA CCDC; 2014
- **Challenge Creator** and Operations; NCL; 2014
- **1st Place** - World Championship; Symantec CRC; 2013
- **1st Place** - Championship Qualifications; Synmantec CRC; 2013
- **Gold Team** and Exercise Operations; MA CCDC; 2013
- **Challenge Creator** and Operations; NCL; 2013
- **2nd Place** - International Champions; Global CyberLympics; 2012
- **1st Place** - North American Champions; Global CyberLympics; 2012
- **1st Place** - Red Cell; MA CCDC; 2012
- **Gold Team** and Exercise Operations; MA CCDC; 2012
- **Challenge Creator** and Operations; NCL; 2012
- **Gold Team** and Exercise Operations; MA CCDC; 2012
- **3rd Place**; MITRE-STEM CTF; 2012
- **Team Captain**; ICF International (Various); 2012
- **2nd Place** - International Champions; Global CyberLympics; 2011
- **1st Place** - North American Champions; Global CyberLympics; 2011
- **1st Place** - Red Cell; MA CCDC; 2011
- **1st Place** - Champion; MDC3; 2011
- **Team Captain**; ICF International (Various); 2011
- **1st Place** - Red Cell; MA CCDC; 2010
- **Team Captain**; ICF International (Various); 2010
- **Red Cell** Member (Invitee); MA CCDC; 2009
- **Team Captain**; ICF International (Various); 2009
- **2nd Place** - Red-Cell; Cyber Dawn; 2009
- **Finalist**; National CCDC; 2008
- **1st Place** - Blue Cell; MA CCDC; 2008
- **Team Captain**; CCBC (Various); 2008
- **2nd Place** - Blue-Cell; MACCDC; 2007
- **Team Captain**; CCBC (Various); 2007
- **3rd Place** - Blue-Cell; MA CCDC; 2006
- **Team Captain**; CCBC (Various); 2008