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

EXPERIENCE

Director; Security Advisory Services Core BTS *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.

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.

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.

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.

Engagement Lead & Researches; 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.

ADDITIONAL EXPERIENCE

Freelance & Consulting		*06/02 - Present*
Warrant Officer	Maryland Defense Force	*05/13 - 05/17*
Adjunct Professor	Comm. College Balt. Co	*10/10 - 01/15*
Security Engineer & Researcher	ICF International	*10/07 - 10/12*
IT Technician	Constellation Energy Grp	*08/06 - 10/07*
Network & Security Administrator	Hi-Tech Processing Svcs	*10/05 - 10/06*

SKILLS & FOCUS

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

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.).

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 Blind (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 (Core BTS)

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

---

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.