WILLIAM I. WINSTON

454 WOODLAWN • YPSILANTI, MI 48198 • (313) 207-3868 • will.winston@gmail.com

APPLICATIONS SECURITY ENGINEER with more than 15 years of experience in **SDLC assessment** and **improvement**, **IT infrastructure maintenance** and **deployments**, **risk analysis**, **threat reporting**, **organizational buy-in**, and **cross-functional leadership**. Analytical and results-oriented **problem solver** with a proven record of **large-scale software deployments** and **security initiatives** designed to **safeguard the enterprise** from prospective compromises. Dedicated **leader** leveraging **interpersonal skills** to **communicate** complex, **intricate concepts** with **key internal stakeholders** and external entities to **ensure mission-alignment** and **execute process improvements**.

AREAS OF EXPERTISE

- ✓ *Application Security*
- ✓ *Network Defense*
- ✓ *Multifunctional Teamwork*
- ✓ *Systems Improvements*
- ✓ *Penetration Testing*
- ✓ *Technology Leadership*
- ✓ *Strategic Planning & Execution*
- ✓ *SDLC Optimization*
- ✓ *Threat & Risk Analysis*

PROFESSIONAL EXPERIENCE & ACCOMPLISHMENTS

Delta Dental of Michigan – Okemos, MI 09/2019 – Present

Senior Application Security Engineer

*Serves as a member of an **application security** team with functions comprising **continuous improvement** for the **software development lifecycle (SDLC)** and directing **critical initiatives** to **enhance the organizational security position**.*

SDLC Improvement:

- Utilized **architecture risk analysis** and **threat models**, **collaborating with team members** over a two-year period to effectively **detect and document prospective vulnerabilities** in the **SDLC design phase**.
    - Developed and **presented a proof of value** with **C-level members**, **securing buy-in** to prioritize **increased funding** for **high-risk applications**.
- Oversaw the **automated web application scan program** in an effort to isolate and **resolve common software exposures**—including **OWASP Top 10**—on **public-facing applications**.
- **Monitored external network** for unauthorized **application deployments**, **ensuring support team** utilization of **established change control processes**.
- Directed requisite **third-party penetrations tests** as well as **conducting internal assessments** on **web applications** to **ensure the protection** of **organizational applications** and **data**.
- **Coordinated with projects teams** regarding **best practices** for the **successful implementation** of controls that **safeguard a layered defense** for **designated applications**.
    - Additionally, **mentored two new** hires by **establishing targets** and **forecasting performance** to **accelerate the training process** and facilitate a **productive acclimation process**.

Risk Analysis & Mitigation:

- Executed mission-critical **risk analysis** on **software** and **network vulnerabilities** isolated during **scans** and **penetration tests** to support in the **prioritization of resources** during the **remediation process**.
- Regularly met with and **communicated with the risk governance committee**, identifying high and very-high risks and **delivering recommendations** for **corrective action** to **senior leadership**.

Vendor Relationship Management:

- Operated as the **primary point of contact** for all **third party service negotiations**, **expanding operational capacity** and **resources** to drive the program forward and **increase efficiency**.

Comerica Bank – Auburn Hills, MI 04/2014 – 09/2019

Senior Information Security Engineer, Vice President

*Served a member of an **application security** team **validating network controls** and **executing risk analysis** for vulnerabilities.*

Network Control Validation:

- Oversaw the system and **network administration**, including **designing internal communications** and managing the **successful execution** of **requisite network tests**.

  - **Specific tests** included yearly **internal and external network** red **team engagement**, **PCI network environment test**, and **SWIFT infrastructure assessment**.
- Architected and integrated an integral **enterprise communication plan**, **coordinating with key stakeholders** and **bolstering transparency** to **safeguard strategic alignment**.
  - **Documented a procedure** for the **rules of engagement** to **ensure common practice** during the **execution of penetration tests**.
- **Championed incident response procedure** and **information security policy reconstitution** throughout the organization, **directing meetings** focused on **implementing recommendations** elicited from tests.

Cloud Infrastructure Integration:

- **Spearheaded institution** of **Shadow IT** and **cloud monitoring** over a two-year period, presenting a **business case** and **securing buy-in** with **leadership** to **increase visibility** in the **cloud infrastructure**.
- Developed and implemented **standard operating procedures (SOPs)** for oversight, **trained internal staff** on **usage**, and served as the **subject matter expert (SME)** to facilitate a successful and **seamless transition**.

University of Michigan – Ann Arbor, MI 04/2002 – 04/2015

OS Programmer Senior

- Served as a key member for a **system support** team overseeing the updating and maintenance of a **Windows computing environment** with more than 6K **computers**, 100K **users**, and 300K **applications**.
- **Coordinated with team members** for **security assurance**, running a consistent **maintenance cycle** and **performing corrective action** as necessary to **mitigate compromises** and **manage risk**.
  - Participated in substantial **information technology (IT) security training** ranging from **coding level coursework** to full **operating system (OS) security**.
- **Performed major deployments** for **software** and settings by utilizing **active directory**, **group policies**, and **system center configuration manager** to **enhance the academic resources** and **experience for users**.
  - **Demonstrated technical leadership** and **expertise** during the **Computer Showcase cash register** and **network firewall deployment** for a **multimillion dollar business**.
- Directed a **key security assessment** for a **substantial component** of the **academic computing environment**, resulting in **improved security standards** and the **development of business continuity plans** regarding **disaster** and **recovery planning**.

UNITED STATES AIR FORCE EXPERIENCE & ACCOMPLISHMENTS

110th Attack Wing – Battle Creek, MI 10/2016 – Present

Cyber Warfare Officer

- Leveraged **network defense** and **technical security expertise** after **receiving a promotion**, leading a **cyber threat emulation team** to **provide requested defense** and **simulate attacks** from a **variety of adversaries**.
- Led **deployments at key military bases** by **conducting critical risk** and **assessments**, **applying mitigation techniques**, **modifying security policies** and **technical configurations**, and **communication high-priority threats** through necessary channels to **support network defense** and **augment response tools**.

180th Fighter Wing – Swanton, OH 01/2014 – 10/2016

Intelligence Officer

- **Assumed command** of an **intelligence team** responsible for **delivering critical intelligence** for the **threat landscape**; received an **excellence award** for **unwavering leadership** and **quality performance** of the unit.

EDUCATION

Master of Science (MS), Network Security: Eastern Michigan University

Bachelor of Science (BS), Computer Science: University of Michigan

CERTIFICATIONS & CLEARANCES

CISSP | GCFA | Top Secret Clearance

ADDITIONAL EDUCATION & TRAINING

SANS 508 | SANS 542 | SANS 555 | SANS 642 | Intelligence Officer Training

Air Force Cyber Warfare Operations | Air Force Cyber Vulnerability Attack and Hunt

Air Force Officer Training School | Automation in AWS | Certified Ethical Hacker