skillrex
Cyber Workforce. Delivered.

women in CYBERSECURITY WiCyS

2026 WiCyS Talent Study

September 2026

Executive Summary

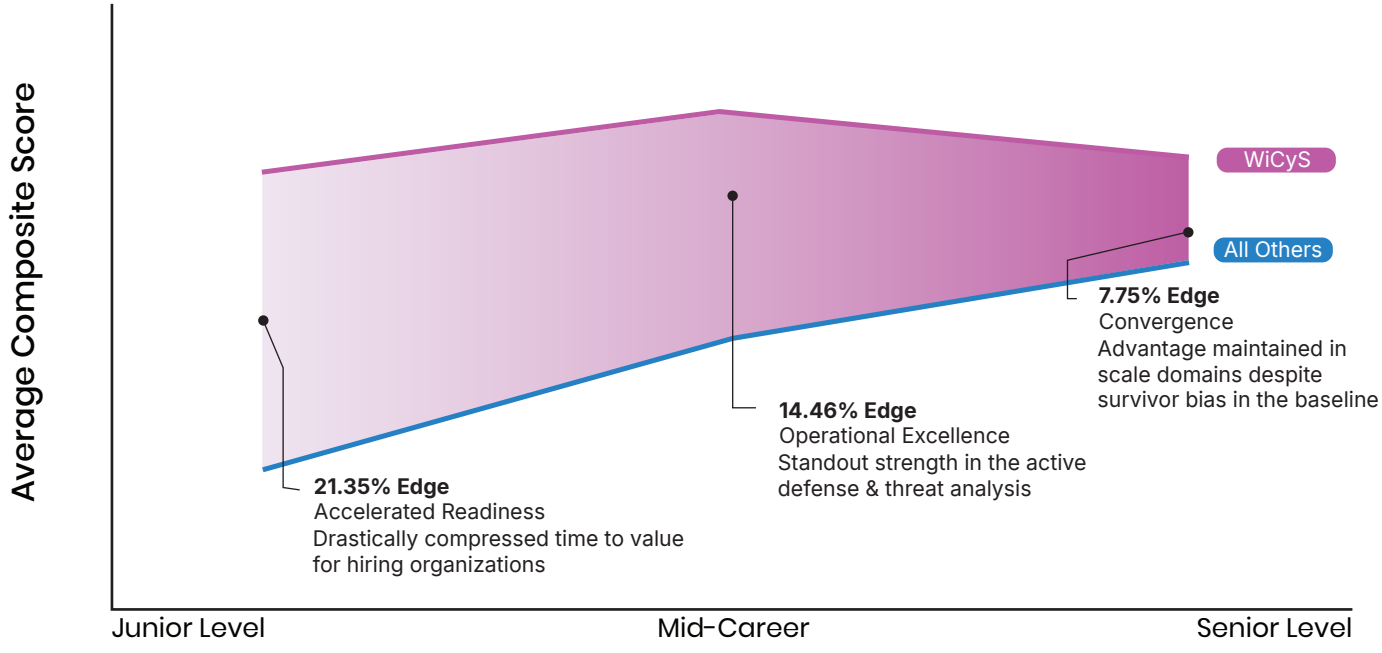
The cybersecurity industry faces a critical transition from legacy, credential-centric recruitment models to dynamic, skills-first talent alignment strategies. In this shifting landscape, the capability profiles of diversely sourced practitioners represent a vital opportunity for organizations seeking to build resilient security programs. This study, a workforce intelligence collaboration between Women in CyberSecurity (WiCyS) and skillrex, provides an empirical look at the performance of women in the cyber workforce.2 By benchmarking 551 WiCyS members against a global cohort of non-WiCyS IT and security practitioners—referred to as All Others—the research maps capability distributions across Technical, Organizational, Professional, and Leadership domains. This analysis isolates where performance edges concentrate, how they evolve across career stages, and where strategic exposure gaps persist.

The primary metric used to quantify these capability profiles is the Performance Edge; calculated as the percentage difference in average composite assessment scores between WiCyS participants and the comparison cohort. Across the entire cohort, WiCyS members demonstrate a robust and systemic performance advantage—referred to as the WiCyS Edge—which averages 14.5% across all experience levels. However, this advantage is highly elastic, exhibiting a clear longitudinal curve as practitioners mature:

- **Junior-Level Edge (21.35%):** Entry-level WiCyS members enter the workforce with significantly elevated capability baselines, particularly in critical thinking, communications, and initial technical readiness, which materially compresses their time-to-value for hiring organizations.
- **Mid-Career Edge (14.46%):** The performance advantage remains substantial as practitioners pivot into complex operational environments, demonstrating standout strengths in vulnerability assessment, threat analysis, and active defense orchestration.
- **Senior-Level Edge (7.75%):** As the comparison cohort gains extensive on-the-job experience and industry attrition exercises a strong survivor bias on the talent pool, the overall score differential compresses. Nonetheless, senior WiCyS leaders maintain clear dominance in human-centric scale domains, such as education delivery, knowledge management, and identity management.

Beyond technical baselines, a critical differentiator is the cohort's signature in Power Competencies. Often referred to in the industry as 'soft skills' or professional employability skills, Power Competencies encompass the non-technical interpersonal, organizational, and leadership attributes required to drive business outcomes. Combining these domains, the WiCyS cohort registered an aggregate average of 55.58 against the industry baseline of 52.66, establishing a 5.53% Performance Edge. In practice, these competencies drive crisis response coordination, cross-functional stakeholder alignment, and strategic risk translation—making them indispensable for resilient security teams.

THE WICYS PERFORMANCE EDGE:
LONGITUDINAL CAREER ANALYSIS



A key workforce planning insight surfaced by this research is what we refer to as the Confidence-Competence Calibration Paradox. Historically, entry-level candidates, especially those sourced from professional associations and academic programs, report highly elevated self-indicated capability profiles. When these aspirational professionals enter the daily realities of active cyber roles, they experience a natural self-assessment calibration. As they confront the hands-on requirements of enterprise security operations, they develop a more realistic understanding of technical execution boundaries. This calibration effect, rather than a decline in capability, explains – in part – the narrowing of the Performance Edge at higher tiers. It highlights why organizations must rely on objective and ongoing, validation-based skills intelligence rather than self-reported resumes when planning pipelines.

A parallel challenge lies in career exposure gaps. Despite strong technical baselines and superior professional skills, the aggregate WiCyS cohort experiences consistent negative margins in commercial leadership functions, including contracting, procurement, supply chain security, and strategic corporate planning. This suggests that female practitioners may face systemic exclusion from executive financial and commercial responsibilities, creating a critical bottleneck in the executive pipeline. Resolving this exposure gap is the next frontier for organizations seeking to convert operational excellence into C-suite leadership.

Comparative Cohort Demographics

To establish a statistically sound foundation, the study benchmarks a diverse group of WiCyS members against a global cohort of non-WiCyS IT and cyber security practitioners, designated as All Others. The total sample consists of 1,332 individual assessment records. The distribution across experience levels highlights different talent pipelines within each cohort:

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	289	150	112	551
All Others	147	346	288	781
Grand Total	**436**	**496**	**400**	**1,332**

This demographic footprint reveals that while the comparison cohort is heavily concentrated in mid-career and senior tiers, the WiCyS population has a highly active entry-level base, representing a significant source of raw talent for the industry.

The Longitudinal Performance Curve

Evaluating the data through an experience-stratified lens reveals how the WiCyS Edge manifests at different career stages, identifying where talent is immediately productive and where development efforts should be focused. The overall aggregate comparison sets a clear baseline:

Competency Domain	WiCyS Aggregate Score	All Others Aggregate Score	Score Difference	Performance Edge
Overall Composite	49.74	47.52	+2.22	4.68%
Professional	74.73	65.09	+9.64	14.81%
Organizational	52.37	50.13	+2.24	4.47%
Technical	45.67	43.93	+1.74	3.96%
Leadership	47.19	49.60	-2.41	-4.86%

This aggregate view underscores that while WiCyS members hold a robust advantage in professional and organizational capabilities, they face persistent deficits in leadership domains. Stratifying this performance by career stage reveals how these margins evolve over time.

Junior-Level: Accelerated Readiness

Entry-level WiCyS members outperform their peers by a margin of 21.35%, reflecting high workforce readiness at the point of entry. This accelerated readiness is concentrated in professional capabilities that are notoriously difficult to develop through traditional technical instruction.

The quantitative metrics for the junior cohort highlight significant advantages across multiple competencies. Twelve of those competencies are highlighted below:

Competency Category	Junior Competency	WiCyS Score	All Others Score	Score Difference	Performance Edge
Professional	Critical Thinking	77.8	52.3	+25.5	48.77%
Professional	Communication	75.9	52.6	+23.3	44.25%
Professional	Conflict Management	67.8	48.0	+19.8	41.24%
Professional	Emotional Intelligence	77.2	57.5	+19.7	34.21%
Organizational	Project Management	54.3	38.7	+15.6	40.34%
Organizational	Risk Management	50.9	37.8	+13.1	34.76%
Organizational	Law, Policy Ethics	47.4	35.1	+12.2	34.76%
Technical	Cloud Security	43.4	32.3	+11.0	34.17%
Technical	Digital Forensics	40.7	30.3	+10.5	34.68%
Technical	Data Analysis	51.7	38.7	+13.0	33.61%
Technical	Computer Languages	52.1	39.7	+12.4	31.39%
Leadership	Strategic Planning	46.0	38.9	+7.1	18.18%

These findings indicate that the onboarding, mentoring, and peer-to-peer support structures in the WiCyS ecosystem provide a strong foundation. This preparation allows junior professionals to contribute to enterprise security objectives much faster than average entry-level hires, effectively lowering onboarding costs.

Mid-Career: Operational Excellence and Career Exposure Gaps

At the mid-career stage, the performance margin narrows to 14.46%. Here, practitioners are deeply integrated into active enterprise defense, security operations centers, and compliance engineering. WiCyS members at this tier show exceptional technical proficiency in vulnerability assessment, threat analysis, and incident management. This technical focus confirms they are heavily involved in defending networks and hardening organizational infrastructure.

However, this operational focus is accompanied by clear deficits in broader organizational and business competencies. Mid-career WiCyS members register negative performance differentials in contracting, procurement, and supply chain security. They also show flat or slightly negative margins in business acumen and strategic relationship management. This divergence suggests a career exposure gap. Female practitioners are often directed into technical engineering and operational compliance roles, leaving them with limited opportunities to participate in the commercial, vendor-facing, and financial aspects of cybersecurity. This exclusion from strategic business functions limits their development and creates a bottleneck when they seek to transition to director and executive roles.

Senior-Level: Convergence with Specialization

At the senior and managerial level, the performance margin compresses to 7.75%, with the senior WiCyS average rising to 56.33 and the industry baseline climbing to 52.28. This compression is a natural result of career maturity, industry attrition, and survivor bias. Over time, practitioners in the comparison cohort gain deep, on-the-job experience, which helps close the capability gaps observed at earlier stages.

At this senior tier, WiCyS leaders show exceptional strength in education training delivery, knowledge management, and identity management. They excel at scaling operational standards, building internal security training programs, and managing identity governance structures across the enterprise.

Yet, the strategic gaps identified at mid-career persist at the senior level. Senior WiCyS members continue to face deficits in strategic planning, contracting, and procurement compared to their male peers. This confirms that the career exposure gap is a structural issue. Without intentional exposure to commercial, procurement, and executive strategy planning, senior female leaders face barriers to entry for C-suite roles, such as the Chief Information Security Officer position.

The Confidence-Competence Calibration Paradox

A key insight identified in this study is the Confidence-Competence Calibration Paradox, which primarily affects early-career professionals. Historical observations in workforce intelligence have noted that junior-level practitioners, particularly those sourced from cybersecurity associations who are still in academic or theoretical programs, self-indicate significantly higher levels of proficiency than junior peers already working in the field.

The underlying mechanism of this paradox is a transition in professional self-awareness:

- **Academic/Aspirational Overconfidence:** While in academic programming or participating in professional networks, junior-level candidates are exposed to structured, idealized security concepts. Lacking the friction of operational enterprise realities, they self-report highly elevated competency levels.
- **Operational Grounding:** When these practitioners secure employment and begin performing the actual duties of their roles, they confront the complexities of enterprise environments—such as legacy infrastructure, configuration dependencies, budget limitations, and organizational politics.
- **Self-Correction and Calibration:** This real-world exposure leads to a cognitive calibration. Practitioners become more realistic about what they do and do not know, leading to more grounded, accurate self-assessments.

This calibration curve is illustrated by the aggregate data, where the performance edge drops from 21.35% at the junior level to 14.46% at mid-career, and ultimately to 7.75% at the senior level. Rather than representing a loss of capability, this compression indicates a maturing of self-assessment and a grounding in operational realities.

For Chief Information Security Officers and workforce leaders, this paradox represents a tricky and potentially significant blind spot. Relying solely on self-reported resumes or unvalidated interviews can lead to mismatched expectations, where entry-level hires are assumed to possess operational capabilities they have only studied theoretically. To build resilient teams, organizations should prioritize skills-based validation instruments—such as the skillrex Baseline Assessment—alongside apprenticeship, internship, and other experiential programs. These initiatives ensure that talent onboarding is grounded in demonstrated capabilities, maximizing training ROI and aligning professional development with actual organizational needs.

Strategic Recommendations for Security and Workforce Leaders

1. Accelerate Junior-Tier Pipeline Integration

The primary cost of junior talent isn't compensation. It's their time-to-value.

The data shows that entry-level WiCyS members bring an immediate 21.35% Performance Edge, concentrated in foundational power competencies like critical thinking and complex problem-solving. This profile directly challenges the assumption that entry-level hires require extensive operational buffering before they can contribute to enterprise environments.

Workforce leaders can compress onboarding timelines by actively sourcing talent from professional networks that provide structured peer mentoring and technical verification platforms. Prioritizing verified readiness over arbitrary job history allows hiring managers to fill critical frontline openings quickly, reducing team burnout and accelerating operational output.

2. Target Commercial and Strategic Development for Mid-Career and Senior Leaders

Technical engineering mastery alone does not build a C-suite pipeline. Exposure does.

The study reveals a systemic bottleneck at the mid-career and senior layers: diverse technical talent consistently matches or exceeds industry baselines in tactical defense, yet experiences a persistent negative margin in commercial leadership loops like contracting, vendor procurement, and corporate strategic planning. This is a clear career exposure gap. High-performing technical women are frequently kept in siloed operational compliance configurations while their peers are rotated into high-visibility financial and commercial responsibilities.

CISOs must intentionally re-engineer leadership development pathways. Moving top technical talent through mandatory business rotations—such as leading third-party risk procurement, managing vendor negotiations, and defending security infrastructure budgets—prepares them for executive roles. Resolving this exposure bottleneck is essential for turning tactical engineering success into long-term enterprise leadership resilience.

3. Transition from Subjective Credentials to Objective Skills Validation

Resumes tell you what someone studied. They rarely tell you what they can execute.

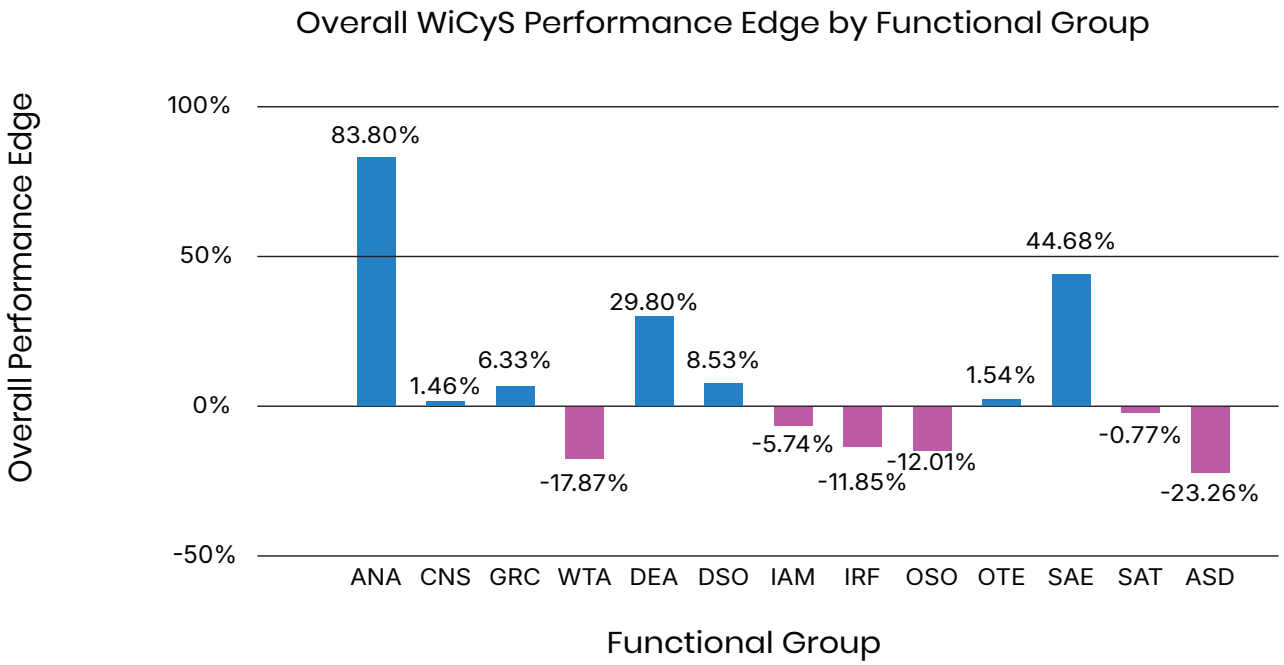
The Confidence-Competence Calibration Paradox proves that unverified self-assessments routinely collapse under the friction of live corporate networks. Aspirational candidates evaluated within purely theoretical frameworks often overrate their initial operational readiness. This disparity creates a major workforce planning blind spot, leading to mismatched performance expectations, high first-year turnover, and misallocated training investments.

Organizations must stop recruiting against unverified job titles, academic degrees, or superficial resume buzzwords. CISOs and talent leaders should implement objective, multi-dimensional skills intelligence across both hiring pipelines and internal development tracks. Validating practical performance capability up front enables organizations to ground self-reported profiles in reality, target specific skill gaps, and optimize overall training returns while protecting enterprise uptime.

1 2025 Cybersecurity Hiring Trends: Why Investing in Entry- and Junior-Level Talent is Key to Building a More Resilient Cybersecurity Workforce - ISC2, accessed July 7, 2026.

Functional Group Dissection

Evaluating talent at the aggregate or career-stage level can hide important details. True workforce intelligence requires looking at how capabilities are distributed across specific functional areas. This section analyzes the thirteen functional groups to show where capability advantages are concentrated, identify talent pools, and locate areas for strategic investment.



The chart above outlines the overall WiCyS Performance Edge across functional groups, aggregating capabilities across all experience levels against industry baselines. The data highlights pronounced performance advantages in specialized technical and analytical domains, led by Analysis (ANA) at +83.80%, Security Architecture & Engineering (SAE) at +44.68%, and Data Engineering & Analytics (DEA) at +29.80%. Conversely, functional groups such as Application Security & Development (ASD) at -23.26% and Workforce, Training & Awareness (WTA) at -17.87% reflect negative performance edges, pointing to primary areas for targeted skill advancement. The following section provides a granular dissection of each functional group to examine how these capability trends shift across specific career stages.

- Analysis
- Communications and Network Security
- Cyber/IT Policy & Governance Risk, & Compliance
- Cyber Workforce, Training, & Awareness
- Data Engineering & Analytics
- Defensive Security Operations
- Identity & Access Management
- Incident Response & Forensics
- Offensive Security Operations
- Operational Technology & Engineering
- Security Architecture & Engineering
- Security Assessments/Testing
- Software/App Security & Secure DevOps

Functional Group	Junior	Mid	Senior	Aggregate
ANA	139.15%	57.79%	172.75%	83.80%
CNS	61.05%	52.11%	-6.67%	1.46%
GRC	33.56%	50.84%	4.24%	6.33%
WTA	-32.44%	-23.04%	-4.34%	-17.87%
DEA	62.06%	63.79%	18.24%	29.80%
DSO	83.87%	7.78%	8.80%	8.53%
IAM	-9.59%	10.54%	-4.58%	-5.74%
IRF	123.61%	-0.04%	-29.75%	-11.85%
OSO	-4.50%	-13.37%	-24.46%	-12.01%
OTE	8.52%	7.19%	-5.90%	1.54%
SAE	134.99%	-45.04%	67.53%	44.68%
SAT	-56.59%	132.75%	2.61%	-0.77%
ASD	-22.42%	-12.23%	-21.69%	-23.26%

A more granular cross-sectional analysis—stratifying Performance Edge by functional group across Junior, Mid-Career, and Senior experience levels—reveals that the WiCyS Edge is highly elastic and non-linear across career stages:

At the entry level, WiCyS members demonstrate extraordinary outperformance in critical frontline functions, led by Analysis (ANA: +139.15%), Security Architecture & Engineering (SAE: +134.99%), Incident Response & Forensics (IRF: +123.61%), Defensive Security Operations (DSO: +83.87%), Data Engineering & Analytics (DEA: +62.06%), and Communications & Network Security (CNS: +61.05%). This dramatic early-stage advantage confirms that entry-level WiCyS talent enters active operational environments with exceptional baseline readiness, enabling hiring organizations to drastically compress onboarding timelines and accelerate time-to-value.

However, as practitioners transition into mid-career and senior tiers, domain-specific trajectory patterns emerge that reflect both professional development and structural career exposure gaps. In governance and testing disciplines like GRC (+33.56% Junior → +50.84% Mid → +4.24% Senior) and Security Assessments & Testing (SAT: -56.59% Junior → +132.75% Mid → +2.61% Senior), performance surges at the mid-career layer as practitioners ground academic/theoretical concepts in live enterprise environments. In contrast, in engineering and defensive operational lanes such as Communications & Network Security (CNS: +61.05% Junior → +52.11% Mid → -6.67% Senior) and Incident Response & Forensics (IRF: +123.61% Junior → -0.04% Mid → -29.75% Senior), as well as Offensive Security Operations (OSO: -4.50% Junior → -13.37% Mid → -24.46% Senior), the score delta compresses or turns negative at senior tiers. This compression highlights both the survivor bias of long-tenured industry comparison cohorts and persistent career exposure gaps that restrict senior female technical talent from accessing executive commercial, procurement, and strategic planning loops.

The following section provides a granular dissection of each functional group to examine how these capability trends shift across specific career stages.

1. ANALYSIS (ANA)

The Analysis functional group is responsible for synthesizing threat telemetry, operational logs, and business intelligence to identify trends and systemic risks across the corporate ecosystem.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	25	13	4	42
All Others	147	15	3	42

Performance Baseline

The quantitative scoring across all experience levels reveals a significant performance advantage for the WiCyS cohort across all competency domains:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	57.74	31.42	26.3	83.80%
Leadership Competencies	54.52	29.53	25.0	84.61%
Organizational Competencies	59.92	31.25	28.7	91.72%
Professional Competencies	77.46	33.87	43.6	128.68%
Technical Competencies	54.59	31.37	23.2	74.03%

Strategic Analysis

The core risk in security analysis teams isn't a lack of alerts. It's an inability to interpret them. Most organizations suffer from an alert-driven loop where tier-1 analysts simply pass indicators up the chain without contextual evaluation.

The data from the Analysis functional group highlights a major difference in how teams process threat data. The WiCyS cohort demonstrates an aggregate 83.80% Performance Edge over the industry control group, showing a systemic ability to connect technical telemetry to business risk.

A deeper look at each experience tier reveals how this advantage develops:

- **Junior Tier (Accelerating Time-to-Value):** The traditional cost of junior hires is determined by how long it takes them to become productive. Junior WiCyS analysts compress this timeline by leveraging a significant advantage in professional competencies. They achieve a critical thinking score of 83.7 against the benchmark's 35.0 (a 139.15% edge) and a communication score of 78.1 compared to 35.4 (a 121.03% edge). Combined with an initial lead in technical execution (39.65 vs. 32.45), these early-career practitioners possess the core competencies required to begin triaging alerts and modeling risks with minimal hand-holding.
- **Mid-Career Tier (Sustaining Technical Dominance):** In many functional groups, mid-career professionals experience a drop in performance as they adjust to corporate realities. However, mid-career WiCyS analysts break this trend by extending their overall advantage to 57.79%. Their performance is anchored by technical outperformance (44.11 vs. 28.73, a 53.55% edge), showing a strong command of modern detection tools. They maintain this edge in key operational areas like Access Controls (55.28 vs. 28.67) and Incident Management (51.11 vs. 27.33), indicating they are highly effective tactical operators.

- **Senior Tier (Strategic Threat Translation):** At the senior layer, the capability gap widens significantly, with WiCyS operators achieving an overall 172.75% performance advantage over the control group. While senior control group practitioners score low across specialized domains, senior WiCyS analysts achieve high marks in critical technical capabilities: Threat Analysis (95.00 vs. 36.67), Intelligence Analysis (90.00 vs. 20.00), and Vulnerabilities Assessment (100.00 vs. 33.33).

This senior tier data suggests that the broader industry analyst pool remains focused on basic, tool-centric monitoring. In contrast, senior WiCyS operators develop into strategic security analysts. They demonstrate the technical capability, organizational context, and leadership alignment needed to help organizations shift from a reactive security posture to proactive, intelligence-driven defense.

2. Communication & Network Security (CNS)

This functional group focuses on designing, implementing, and securing communication architectures and enterprise network boundaries.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	5	4	11	20
All Others	24	68	46	138

Performance Baseline

The quantitative scoring across all experience levels reveals that while the aggregate baseline differences between the cohorts appear marginal, substantial performance deltas exist when the data is stratified by experience tier:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	55.07	54.28	0.79	1.46%
Leadership Competencies	49.63	54.98	-5.35	-9.73%
Organizational Competencies	51.40	53.42	-2.02	-3.78%
Professional Competencies	71.76	67.96	3.79	5.58%
Technical Competencies	55.33	52.98	2.35	4.43%

Strategic Analysis

A top-heavy engineering team is an endangered enterprise asset. In network security, companies routinely rely on a small pool of veteran administrators who understand the physical perimeter but are completely disconnected from modern software-defined architectures.

The participant distribution within the Communication & Network Security domain highlights this exact vulnerability. The industry control group is deeply back-loaded, containing a combined 114 mid-career and senior operators compared to a minimal early-career baseline. This deep bench of veteran industry professionals gives the control group its performance advantage at the senior layer, where senior WiCyS operators lag by **-6.67%** overall.

However, evaluating the early-stage talent pipeline turns this narrative completely upside down:

- **Junior Tier (Redefining Transit Readiness):** Early-career control group practitioners are failing to keep pace with the baseline requirements of modern corporate networks. Junior WiCyS members completely outperform them, securing a 61.05% overall Performance Edge. This outperformance is driven by an exceptional 70.56% advantage in core technical execution (54.70 vs. 32.07). Where the industry baseline drops to critically low performance levels, junior WiCyS operators show immediate, practical mastery in zero-trust enablers, such as Cloud Security (65.00 vs. 31.38, a **107.14%** edge) and Access Controls (65.00 vs. 32.76, a **98.42%** edge). They enter the field fully equipped to manage software-defined network layers with zero initialization lag.

- **Mid-Career Tier (Sustaining the Velocity):** This momentum continues directly into the mid-career layer. Mid-career WiCyS operators maintain a commanding 52.11% overall Performance Edge, backed by a **45.11%** advantage in technical capabilities (48.44 vs. 33.38). These practitioners excel in critical foundational routing and perimeter logic, securing high marks in Network Management (60.00 vs. 34.05, a **76.22%** edge) and Access Controls (66.67 vs. 35.24, an **89.19%** edge).

- **Senior Tier (The Leadership Exposure Bottleneck):** At the senior layer, the technical delta between the cohorts narrows to near parity (58.30 vs. 59.73). The real divergence occurs in high-level business governance, where senior WiCyS operators face steep deficits in Strategic Planning (42.86 vs. 73.06) and Workforce Management (42.86 vs. 54.54).

This senior-tier deficit is a classic operational exposure gap. Senior women in network engineering are held back by an institutional bottleneck, remaining restricted to tactical perimeter configurations while their male peers are consistently rotated into financial, planning, and organizational leadership loops.

For workforce planners, the operational takeaway is clear. The industry benchmark pool is highly top-heavy and approaching a wave of retirements in legacy infrastructure positions. Organizations can build long-term architecture resilience by actively sourcing talent from the high-performing junior and mid-career WiCyS pools and intentionally breaking down the exposure barriers that prevent senior technical women from taking on enterprise strategic planning roles.

3. Cyber IT Policy & Governance, Risk, & Compliance (GRC)

This functional group is responsible for translating statutory and regulatory requirements into corporate policies, assessing enterprise systemic risks, and maintaining continuous compliance frameworks across the organization.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	53	21	19	93
All Others	29	62	31	122

Performance Baseline

The quantitative performance across all experience levels indicates strong capability alignment between the cohorts, with the WiCyS cohort maintaining a steady operational advantage across every core competency domain:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	49.68	46.72	2.96	6.33%
Leadership Competencies	54.49	53.58	2.91	5.44%
Organizational Competencies	57.38	52.79	4.59	8.69%
Professional Competencies	77.35	67.60	9.74	14.41%
Technical Competencies	41.97	40.62	1.35	3.31%

Strategic Analysis

Corporate GRC teams often face structural pressures to focus on administrative compliance, which can sometimes create a disconnect between policy development and the underlying technical infrastructure. This traditional, checklist-driven approach can unintentionally isolate policy writers from security engineering, hindering the development of holistic, integrated security frameworks.

The data from the Cyber IT Policy & GRC functional group demonstrates a shift away from this disconnect. The WiCyS cohort shows an aggregate **6.33%** overall Performance Edge over the industry control group, demonstrating that governance can be managed as an analytical, security-first discipline rather than an administrative hurdle.

A deeper dive into the stratified career milestones reveals where this edge concentrates and how it matures:

- **Junior Tier (Modern Technical Agility):** Early-career WiCyS GRC specialists enter the field with a comprehensive approach to risk, securing a 34.81% overall Performance Edge. Rather than focusing exclusively on basic documentation, these junior professionals exhibit significant technical curiosity and agility. They outpace the industry baseline by large margins in high-growth, technically demanding domains, including Digital Forensics (38.29 vs. 8.49, a 351.13% edge) and Ai Security (39.52 vs. 21.11, an **87.18%** edge). At the same time, they display strong business alignment skills, leading in Strategic Policy Development (49.40 vs. 22.87, a **116.02%** edge) and Strategic Planning (48.81 vs. 23.15, a **110.84%** edge). This profile indicates that junior WiCyS talent enters GRC roles fully capable of analyzing complex technical architectures and mapping policies to modern cloud and machine-learning environments.

- **Mid-Career Tier (Bridging the Structural Silos):** At the mid-career layer, the WiCyS cohort maintains a strong **29.38%** overall advantage, supported by a **28.57%** edge in technical profile capabilities (46.80 vs. 36.40). These mid-career professionals function as critical translators within the enterprise, combining high professional enablers (**33.45%** edge) with practical risk management skills to bridge the gap between engineering teams and continuous compliance mandates. Their organizational scores are further strengthened by a clear advantage in Supply Chain Management Security (37.54 vs. 20.74, an **80.99%** edge), highlighting their ability to evaluate third-party vendor risks with deep operational understanding.

- **Senior Tier (Strategic Risk Translation):** Senior WiCyS GRC leaders sustain a dominant positioning with a **32.25%** overall Performance Edge and a standout **35.10%** lead in senior technical profiling (61.20 vs. 45.30). Backed by an aggregate **14.41%** professional competencies edge across all levels, these senior leaders possess the communication skills, business context, and structural capability required to translate complex technical vulnerabilities into financial risk metrics for C-suite and board-level leaders.

For CISOs and workforce strategists, the implications of this data are clear. The traditional approach of hiring pure administrative writers for compliance teams creates a major operational blind spot. The deep talent pool within the WiCyS GRC cohort—which accounts for nearly 17% of the total WiCyS sample—represents a highly technical, risk-aware resource. Organizations should intentionally leverage this pipeline to transform their GRC function from a reactive, checklist-driven activity into a proactive risk-advisory service that secures digital transformation initiatives and product delivery pipelines from day one.

4. Cyber Workforce, Training & Awareness (WTA)

This functional group is tasked with building cybersecurity curriculum, delivering enterprise training, managing workforce metrics, and fostering a security-conscious organization.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	27	36	23	86
All Others	12	22	13	47

Performance Baseline

The aggregate performance analysis across all experience levels reveals a distinct pattern where the comparison cohort holds an advantage in technical and leadership domains, while the WiCyS cohort establishes clear parity in professional capabilities:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	39.52	48.12	-8.60	-17.87%
Leadership Competencies	50.02	62.27	-12.25	-19.68%
Organizational Competencies	48.67	57.86	-9.19	-15.88%
Professional Competencies	79.25	78.14	1.11	1.42%
Technical Competencies	29.32	38.48	-9.16	-23.80%

Strategic Analysis

Most organizations don't have a training delivery problem. They have a training relevance problem. The data from the Cyber Workforce, Training & Awareness functional group reveals a critical leadership blind spot: the decoupling of training developers from the active technical infrastructure they are supposed to educate.

When curriculum designers cannot speak the language of engineering, training modules default to generic compliance checklists rather than actionable defense skills.

A deeper dive into the stratified career stages explains this dynamic and shows how to fix it:

- **Junior Tier (The Technical Disconnection):** The significant entry-level overall deficit (**-32.44%**) is a clear structural indicator. Junior control group practitioners are likely sourced from standard IT operations roles, giving them a heavy advantage in day-to-day enterprise governance basics, such as Asset Management (63.33 vs. 37.08) and Workforce Management (61.67 vs. 38.42). Conversely, entry-level WiCyS members in this group show high capability in human-centric domains but lack exposure to production systems, resulting in a low DevSecOps score (19.97 vs. 51.67). However, they possess a strong foundation in problem-solving, leading in Critical Thinking with an 84.44 average against 73.33 for the control group (a **15.15%** edge). This suggests these junior practitioners are highly analytical communicators or HR specialists who have been placed into security education roles without technical onboarding.

- **Mid-Career Tier (The Transition Bottleneck):** This technical gap persists into the mid-career tier, where WiCyS practitioners face a **-28.74%** performance gap in core technical profile execution (31.00 vs. 43.50). This highlights an ongoing barrier to growth: if mid-career training specialists are not rotated into active operational security roles, their understanding of modern infrastructure remains frozen, limiting their ability to build high-impact enterprise curricula.

- **Senior Tier (The Path to Leadership Recovery):** At the senior layer, the overall performance gap almost entirely disappears, narrowing to just **-4.34%**. Senior WiCyS workforce professionals successfully close the distance by establishing clear advantages in Leadership Competencies (65.62 vs. 63.33) and Organizational Competencies (60.12 vs. 58.39). They exhibit high capability in scaling operational standards across the enterprise, driven by strong marks in Workforce Management (71.20 vs. 52.88) and Risk Management (66.67 vs. 48.94).

For workforce strategists, the data highlights a clear action item. Training teams require the exact same data-driven visibility that security infrastructure teams receive. Organizations cannot expect to build a security-conscious workforce if their educators lack technical grounding.

By implementing structured cross-training programs that help non-technical educators master foundational engineering concepts—such as cloud configurations and IT asset management—enterprises can significantly maximize their training ROI and improve overall workforce readiness.

5. Data Engineering & Analytics (DEA)

This functional group is dedicated to managing the end-to-end data lifecycle—encompassing data collection, transformation, pipeline management, storage architectures, and analytic engines that process massive enterprise security logs to power SIEM and active defense environments.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	9	6	4	19
All Others	10	24	9	43

Performance Baseline

The quantitative scoring across all experience levels reveals an exceptional capability advantage for the WiCyS cohort, establishing a commanding Performance Edge in professional log parsing, pipeline architecture, and structural data governance:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	53.95	41.57	12.38	29.80%
Leadership Competencies	46.46	41.25	5.21	12.63%
Organizational Competencies	56.28	41.89	14.39	34.36%
Professional Competencies	71.14	50.50	20.65	40.88%
Technical Competencies	51.42	40.35	11.06	27.41%

Strategic Analysis

Modern security teams don't suffer from a lack of data; they drown in it. The core risk in contemporary SOC and SIEM operations is pipeline inefficiency—treating data engineering as a generic IT function rather than a foundational security baseline. When data pipelines are engineered without security awareness, organizations end up with delayed threat visibility, unparsed log telemetry, and massive ingestion bills.

The data from the Data Engineering & Analytics functional group reveals a distinct structural advantage for the WiCyS cohort. Generating an aggregate **29.80%** overall Performance Edge and a robust **27.41%** outperformance in core technical execution, WiCyS data professionals demonstrate a security-first approach to telemetry pipelines. Rather than treating log management through a generic business intelligence lens, they analyze data with a native understanding of structural risk and threat isolation.

An evaluation of the stratified career stages exposes a critical retention leak alongside a major competitive sourcing opportunity:

- **Junior Tier (Immediate Technical Contributor):** The entry-level cohort features balanced representation (9 WiCyS vs. 10 All Others), pointing to a healthy incoming pipeline. Junior WiCyS data professionals outpace the benchmark group with a **17.45%** technical Performance Edge (49.80 vs. 42.40). Instead of requiring lengthy, basic training on query logic or schema management, these entry-level professionals enter the workforce ready to immediately support log ingestion architectures and structured data lifecycle management.

- **Mid-Career Tier (The Volume Contraction):** As practitioners transition to the mid-career layer, the overall score compresses to statistical parity, and the technical edge narrows to **6.95%** (52.30 vs. 48.90). Crucially, this compression coincides with a stark demographic drop-off: the benchmark control group expands significantly to 24 practitioners, while the WiCyS cohort shrinks down to just 6. This volume contraction signals a leaky pipeline. Mid-career technical women in data roles are frequently funneled into generic project management, data governance documentation, or administrative scheduling rather than being assigned core engineering tasks like scaling ingestion infrastructure or building automated detection models.

- **Senior Tier (Strategic Architecture Mastery):** For the selective pool that breaks through the mid-career bottleneck, capability metrics skyrocket. Senior WiCyS data engineers establish a comprehensive **25.93%** overall Performance Edge, backed by a **26.97%** lead in senior technical execution (67.80 vs. 53.40) and a massive **44.59%** advantage in organizational competencies. These senior leaders excel at parsing complex, unstructured data streams and translating raw data lakes into actionable security intelligence to support cross-functional enterprise objectives.

For CISOs and data infrastructure leaders, this functional group represents a high-leverage opportunity. As enterprises rapidly deploy Large Language Models (LLMs), centralized data lakes, and automated analytics engines, security data engineering has become a critical requirement.

To capitalize on this capability profile, workforce leaders must deliberately re-engineer the mid-career career pathway. Organizations must transition female data professionals out of entry-level pipeline management and actively support their development into platform architects. Preserving this talent pool ensures that future AI integration, security log aggregation, and pipeline analytics are built on clean data architectures that minimize threat exposure and eliminate baseline visibility gaps before they impact production environments.

6. Defensive Security Operations (DSO)

Defensive Security Operations teams focus on protecting corporate networks from unauthorized access, monitoring enterprise environments, detecting active threats, triaging security alerts, and running the corporate Security Operations Center (SOC).

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	40	14	6	60
All Others	7	69	56	132

Performance Baseline

The aggregate performance metrics across all experience levels show strong baseline capabilities for the WiCyS cohort, establishing a clear operational advantage particularly within leadership and professional execution:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	45.40	41.83	3.57	8.53%
Leadership Competencies	45.01	36.31	8.69	23.94%
Organizational Competencies	45.56	44.65	0.91	2.04%
Professional Competencies	81.62	61.09	20.53	33.60%
Technical Competencies	40.96	38.63	2.33	6.04%

Strategic Analysis

The biggest operational bottleneck in defensive security isn't alert volume. It's treating your Security Operations Center as an assembly line of manual button-pushers. Most enterprise leaders face a compounding high-churn loop because they hire entry-level analysts who lack the critical thinking required to investigate threat context, leading to catastrophic alert fatigue and missed indicators.

The Defensive Security Operations data presents a striking competitive sourcing advantage for forward-looking CISOs. The overall metrics show a clear, aggregate **8.53%** Performance Edge for the WiCyS cohort. What makes this outperformance significant is the stark demographic inversion between the groups. While the industry benchmark pool is heavily top-heavy —concentrating 125 out of its 132 practitioners in mature operational tiers— the WiCyS cohort is highly front-loaded, with 40 out of 60 participants situated at the junior layer. Despite this entry-level concentration, the WiCyS group outscores the control pool, pointing to an exceptionally high foundational capability baseline.

A targeted analysis of the stratified career tiers highlights where this advantage delivers direct enterprise impact:

- **Junior Tier (De-risking the Escalation Trap):** The entry-level control group is struggling with a low overall score of 24.03, indicating that standard industry pipelines are producing entry-level hires who lack baseline readiness. Junior WiCyS operators answer this challenge with a massive **83.87%** overall Performance Edge, anchored by a **132.12%** outperformance in professional enablers and an **87.24%** lead in core technical competencies. These early-career analysts bring strong analytical maturity to the team, outclassing the baseline in Critical Thinking (81.30 vs. 31.43, a 158.67% edge) and Strategic Planning (48.52 vs. 22.86, a **112.27%** edge). In practical execution lanes, they possess strong capabilities in modern cloud monitoring environments, leading in Cloud Security (45.56 vs. 22.86, a **99.31%** edge) and Access Controls (51.85 vs. 24.29, a **113.51%** edge). This means a junior WiCyS analyst can immediately begin triaging complex alerts, hunting threat behaviors, and making objective recommendations, reducing the time-to-value for hiring organizations.

- **Mid-Career Tier (Sustaining Incident Velocity):** This operational edge remains solid at the mid-career layer, with the WiCyS cohort establishing a 10.45% overall Performance Edge over the benchmark group. These practitioners are effective active defense operators, showing high proficiency in security infrastructure orchestration and event monitoring.

- **Senior Tier (Driving Resilient Defense Blueprinting):** At the senior layer, the WiCyS cohort maintains an **11.63%** overall edge and a **10.33%** outperformance in senior technical profiling (59.80 vs. 54.20). Supported by a strong aggregate **23.94%** Leadership Competencies edge, these senior operators possess the cross-functional communication skills and technical authority needed to redesign detection architectures, build internal resilience, and manage the SOC during high-stress crisis response events.

For security and workforce leaders, the takeaway is highly actionable. Relying on an expensive lateral hiring market for senior SOC professionals is a temporary fix for a structural problem. The high capability scores of the entry-level WiCyS cohort demonstrate a ready-made solution to the industry tier-1 talent shortage. CISOs can build scalable, long-term operational resilience by intentionally hiring from this high-performing junior pipeline, introducing analysts who possess the cognitive skills and modern cloud security baselines required to handle advanced threat triage early in their careers.

7. Identity & Access Management (IAM)

This functional group is responsible for establishing, managing, and monitoring user identities, single sign-on (SSO) architectures, multi-factor authentication (MFA), directory federation, credential management, and role-based access controls (RBAC) to ensure authorized individuals and entities have appropriate access to enterprise resources at the correct time.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	16	4	9	29
All Others	11	33	66	110

Performance Baseline

The aggregate performance baseline highlights an apparent marginal deficit for the WiCyS cohort across aggregate domains, masked heavily by a steep longitudinal divergence in senior industry composition:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	56.20	59.62	-3.42	-5.74%
Leadership Competencies	58.10	69.40	-11.30	-16.28%
Organizational Competencies	62.57	65.50	-2.92	-4.46%
Professional Competencies	80.18	72.02	8.16	11.33%
Technical Competencies	50.02	54.38	-4.35	-8.01%

Strategic Analysis

Relying on legacy Active Directory configurations while building a zero-trust architecture is a recipe for operational failure. In identity management, many organizations suffer from a structural blind spot: treating identity as an isolated administrative support ticket center rather than the primary defense perimeter of cloud infrastructure. When identity platforms are built on manual provisioning and outdated, siloed configurations, they become an open door for lateral movement during threat actor incursions.

The raw aggregate data for the Identity & Access Management functional group presents an initial, misleading data profile. On the surface, the WiCyS cohort registers an apparent overall baseline deficit of -5.74%. However, this overall dip is a classic example of demographic skew masking operational reality. The industry control group is deeply top-heavy, containing a massive base of 66 senior professionals out of 110 total participants. Conversely, the WiCyS cohort is highly front-loaded, with over 55% of its population concentrated in the junior tier. This sharp difference in career longevity naturally depresses the combined WiCyS average.

When we strip away this composition imbalance and look at the data stage-by-stage, a highly competitive talent strategy emerges:

- **Junior Tier (Injecting Cloud-Native Perimeters):** The early-career control pool enters the workforce with low overall performance readiness (38.40). Junior WiCyS practitioners address this capability gap by establishing a **20.31%** overall Performance Edge, backed by a **17.45%** advantage in initial technical execution (42.40 vs. 36.10). In contrast to entry-level hires who have to unlearn on-premises, perimeter-based server administration paradigms, these junior WiCyS professionals show high baseline readiness in core zero-trust drivers. They score strong marks in Identity Management (45.30 vs. 37.50, a **20.79%** edge) and Access Controls (55.00 vs. 33.79, a **62.76%** edge). This positioning creates an immediate sourcing opportunity to fast-track modern cloud directory federation projects with minimal onboarding overhead.

- **Mid-Career Tier (Navigating the Volume Bottleneck):** As practitioners pivot into the mid-career layer, the WiCyS performance edge settles at a positive **7.74%** overall advantage. However, the sample sizes show a significant retention bottleneck: the benchmark cohort contains 33 mid-career professionals, while the WiCyS group drops to just 4 active participants. This sharp volume contraction highlights a major workforce risk. Technical women in IAM at this transition point are frequently steered away from active directory synchronizations and security engineering. Instead, they are often directed into compliance documentation or routine professional enabling lanes (52.77% edge), which stalls their technical trajectory.

- **Senior Tier (Strategic Zero-Trust Governance):** For the selective group that advances past the mid-career hurdle, true technical maturity becomes highly visible. Senior WiCyS IAM experts achieve a **16.21%** overall Performance Edge, driven by a **16.26%** outperformance in senior technical profile execution (61.50 vs. 52.90). These senior leaders maintain structural authority in managing advanced access perimeters, outpacing their industry peers in core configuration fields like Identity Management (35.91 vs. 33.94) and Access Controls (50.00 vs. 53.63).

For enterprise security architects and talent strategists, this data provides an actionable path forward. The legacy control group's talent is anchored in aging configurations that are rapidly approaching obsolescence.

By intentionally investing in the high-performing junior WiCyS pipeline and providing them with advanced training in cloud identity frameworks (such as OAuth federation, API security, and directory synchronization architecture), organizations can build modern, automated identity practices. This approach moves the identity function past baseline ticket administration and turns it into a responsive, zero-trust perimeter enabler that secures digital assets and product lifecycles across the entire enterprise.

8. Incident Response & Forensics (IRF)

This functional group is responsible for protecting the enterprise in the event of an active security breach, establishing fast containment protocols, preserving digital chain of custody evidence, analyzing file system and memory artifacts, and coordinating response loops with internal and external legal, operational, and regulatory stakeholders.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	37	12	8	57
All Others	3	8	18	29

Performance Baseline

The aggregate performance baseline highlights an apparent overall capability deficit for the WiCyS cohort, a structural anomaly caused directly by an extreme longitudinal distortion in cohort composition:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	40.00	54.38	14.38	83.80%
Leadership Competencies	32.39	46.68	14.29	-33.46%
Organizational Competencies	41.82	47.60	-5.78	-12.14%
Professional Competencies	64.69	59.97	4.72	7.88%
Technical Competencies	36.82	42.23	-5.41	-12.82%

Strategic Analysis

When an advanced persistent threat (APT) hits your production infrastructure, you don't need a manager reading a policy manual. You need an operator who knows how to dump memory, isolate host communications, and preserve forensic artifacts without blowing up system dependencies. Yet, most organizations treat Incident Response (IR) as an exclusive club of senior gatekeepers, creating a critical shortage of early-career responders capable of performing baseline forensic analysis.

The macro-level baseline for the Incident Response & Forensics group initially highlights a significant capability gap, showing a **-11.85%** overall drop and a **-12.82%** technical deficit for the WiCyS population. However, this aggregate drop is an illusion caused entirely by a severe demographic imbalance. Nearly 65% of the WiCyS cohort consists of entry-level practitioners (37 out of 57), while the industry control pool is heavily top-heavy, concentrating over 62% of its practitioners at the senior level (18 out of 29). This structural skew naturally suppresses the combined WiCyS average.

When we evaluate the talent pool on a tier-by-tier basis, the raw data reveals an impressive pipeline story:

- **Junior Tier (De-risking the Frontline Pipeline):** The broader industry control pool has failed to build an early-career pipeline, showing a tiny group of only 3 junior participants. WiCyS answers this industry shortage by introducing a robust pipeline of 37 early-career practitioners who outperform the baseline by **16.62%** overall. In core tactical and defensive lanes, these junior WiCyS responders outclass the baseline by a staggering margin in Data Security (52.43 vs. 13.33, a **293.25%** edge). They also show strong business alignment skills, leading in Strategic Relationship Management (53.14 vs. 23.33, a **127.73%** edge) and Risk Management (54.88 vs. 10.00, a **448.80%** edge). This means that junior WiCyS responders possess the specific cognitive skills and data mapping baselines required to handle active containment loops and stakeholder communications from day one.

- **Mid-Career Tier (Sustaining Forensic Drift):** As practitioners mature into the mid-career layer, the performance delta reaches a stable **3.52%** overall edge. These operators establish technical parity with the benchmark group while maintaining a clear, steady lead in professional enablers (**11.41%** edge), ensuring that incident coordination loops remain functional under high crisis pressure.

- **Senior Tier (The Leadership Exposure Bottleneck):** At the senior layer, senior WiCyS operators show clear mastery in tactical execution, securing a narrow performance edge in core Digital Forensics (48.91 vs. 48.06, a **1.76%** edge). However, a significant gap appears in senior Leadership Competencies (**-17.79%** deficit). This represents a classic operational career exposure gap: senior technical women in IR are routinely kept in hand-on, deep forensic investigation roles while their male peers are consistently rotated into corporate disaster recovery budgeting, steering committees, and crisis governance leadership lines.

For enterprise cyber leaders, the strategic takeaway is straightforward. The traditional approach of buying expensive lateral senior hires for IR teams is a short-term fix that ignores long-term pipeline collapse. The large talent concentration inside the junior WiCyS cohort represents a massive, highly technical resource that already possesses an established baseline in digital evidence preservation and risk mitigation frameworks.

By intentionally pairing these entry-level professionals with veteran responders and consciously breaking down the exposure bottlenecks that prevent technical senior women from leading executive-level incident loops, CISOs can build a resilient, scalable, and cross-functional incident response engine.

9. Offensive Security Operations (OSO)

This functional group focuses on advanced exploitation techniques, attack simulation, threat emulation, adversary hunting, and bug bounty programs. These activities shift past routine automated vulnerability scanning to focus on multi-stage tactics, techniques, and procedures (TTPs) designed to gain initial access, execute lateral movement, and complete action-on-objectives within an operating environment.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	30	14	5	49
All Others	6	13	14	33

Performance Baseline

The aggregate performance metrics across all experience levels show an apparent advantage for the comparison group, heavily influenced by a demographic skew where the benchmark pool contains a far higher proportion of senior operators:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	51.66	58.71	-7.05	-12.01%
Leadership Competencies	45.33	58.02	-12.69	-21.87%
Organizational Competencies	51.52	58.83	-7.31	-12.42%
Professional Competencies	75.59	77.93	-2.34	-3.00%
Technical Competencies	49.40	56.39	-6.99	-12.39%

Strategic Analysis

A penetration test that only lists unpatched legacy servers isn't an offensive strategy. It is an administrative expense. Historically, offensive security has favored the lone hacker hunting for isolated software exploits.

Modern enterprise environments are cloud-native and platform-driven. This shift means that modern red-teaming requires an understanding of legal boundaries, cloud access misconfigurations, and machine learning structures rather than legacy buffer overflows.

The raw aggregate data for the Offensive Security Operations domain shows an apparent overall deficit of -12.01% for the WiCyS cohort. This is a clear case of demographic skew masking a major pipeline transition. The WiCyS population is highly junior-centric, with 30 out of 49 participants situated at the entry level. Conversely, the comparison group features a mature, top-heavy footprint with 14 senior practitioners.

When we evaluate the data through a stratified, skills-first lens, a clear capability migration becomes visible:

- **Junior Tier (The Modern Attacker Profile):** While entry-level WiCyS offensive specialists score 55.79 overall compared to 58.42 for the comparison group (**-4.50% edge**), they establish a decisive lead in professional enabling competencies (**+6.99% edge**) and future-facing technical execution lanes. Junior WiCyS operators outscore their industry peers in core professional enablers, including Communication (78.33 vs. 62.86, a +24.62% edge) and Critical Thinking (81.25 vs. 74.29, a +9.37% edge). In technical domains, they show significant leads in next-generation attack surfaces: Cloud Security (52.08 vs. 42.86, a **+21.53% edge**), AI Security (54.17 vs. 45.71, an **+18.49% edge**), Law, Policy & Ethics (63.33 vs. 51.43, a **+23.15% edge**), Software Development (60.42 vs. 45.71, a +32.16% edge), and DevSecOps (51.25 vs. 42.86, a **+19.58% edge**). While they show a gap in legacy Vulnerability Assessment (60.00 vs. 74.29, a **-19.23%** deficit), their focus is trained on modern software-defined architectures.

- **Mid-Career Tier (Tactical Leadership & Governance Strength):** At the mid-career layer (48.78 vs. 56.31 overall; a **-13.37% deficit**), WiCyS operators establish a slight edge in Leadership Competencies (48.17 vs. 47.78, a **+0.81% edge**). They demonstrate strong operational governance and tactical execution, leading in Policy Development (47.00 vs. 40.00, a **+17.50% edge**), Organizational Awareness (55.50 vs. 33.33, a +66.50% edge), Incident Management (53.00 vs. 43.33, a **+22.31%** edge), Operations Support (47.50 vs. 40.00, a **+18.75% edge**), and Digital Forensics (45.00 vs. 40.00, a **+12.50% edge**).

- **Senior Tier (Specialized Mastery & Executive Volume Bottleneck):** At the senior layer (45.03 vs. 59.61 overall; a -24.46% deficit), WiCyS operators demonstrate specialized tactical mastery in core assessment disciplines, outscoring their senior industry peers in Threat Analysis (68.00 vs. 63.66, a **+6.82%** edge) and Vulnerabilities Assessment (80.00 vs. 76.48, a **+4.60%** edge). However, the segment suffers from a severe volume restriction, with only 5 senior WiCyS participants compared to 14 in the benchmark pool (a 2.8x volume deficit). This sharp drop-off points to a major retention and promotion bottleneck: senior women in offensive security are frequently restricted to tactical exploit execution rather than being promoted to direct enterprise-wide threat emulation programs or lead purple-teaming initiatives.

For CISOs and workforce strategists, the implications are tactical and immediate. Sourcing offensive talent from traditional, checklist-driven testing pools creates a major blind spot when migrating to cloud and AI-driven environments. The incoming WiCyS offensive pipeline represents a code-fluent, policy-aware cohort focused on testing cloud-native assets, evaluating AI model boundaries, and operating within legal compliance guardrails. Integrating this talent and creating clear pathways for mid-career and senior operators to direct threat emulation programs allows organizations to move past chaotic vulnerability hunting and establish continuous security posture validation.

10. Operational Technology & Engineering (OTE)

This functional group is responsible for managing and securing industrial control systems (ICS), supervisory control and data acquisition (SCADA) platforms, programmable logic controllers (PLCs), manufacturing pipelines, and distributed Internet of Things (IoT) deployments to maintain physical reliability and kinetic safety boundaries across critical infrastructure.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	6	3	2	11
All Others	4	7	4	15

Performance Baseline

The aggregate performance baseline highlights near parity between the cohorts, masked heavily by an industry-wide data volume drought that creates high statistical sensitivity across all experience milestones:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	56.60	55.74	0.86	1.54%
Leadership Competencies	50.00	62.35	-12.35	-19.81%
Organizational Competencies	60.51	54.60	5.92	10.83%
Professional Competencies	74.44	73.12	1.33	1.81%
Technical Competencies	53.13	53.58	-0.45	-0.84%

Strategic Analysis

An open network switch on a factory floor is a risk that cannot be patched with an endpoint agent. In Operational Technology (OT) security, organizations routinely face a structural disconnect: traditional enterprise security teams try to enforce software-defined compliance rules on legacy industrial architectures where an unexpected system reboot can freeze a water treatment facility or halt an assembly line. This specialization gap isn't just about short staffing—it's a failure to translate concepts between IT security practitioners who think in software code and physical systems engineers who manage kinetic safety boundaries.

The workforce demographics for the Operational Technology & Engineering group confirm that talent scarcity is a systemic issue across the entire sector. With single-digit participant counts recorded at every individual career tier for both populations (encompassing a minimal grand total of only 26 individuals), finding qualified operators is exceptionally difficult. While the aggregate data indicates marginal overall parity (**1.54%** Performance Edge), looking at the stratified capability metrics reveals how specialized technical domain mastery is distributed across experience levels:

- **Junior Tier (The Technical Entry Friction):** Sourcing entry-level talent into physical security pipelines requires overcoming significant initial friction. Junior WiCyS practitioners trail the baseline control group in early-stage technical performance by **-3.04%** (31.90 vs. 32.90). This minor deficit points to a lack of early access to specialized hardware labs, industrial control protocols, and physical telemetry testbeds within academic environments. However, these junior practitioners counter this gap by outperforming their peers in Organizational Competencies (**16.72%** edge), demonstrating an immediate ability to map risk compliance mandates and safety rules onto complex physical infrastructure.

- **Mid-Career Tier (The Tactical Technical Inflection):** At the mid-career transition layer, a massive technical inflection occurs. Mid-career WiCyS professionals establish a staggering **42.71%** technical performance advantage over the industry control group (38.06 vs. 26.67). This outperformance stems from clear, practical mastery of specialized industrial networks, outscoring the control pool in OT Security (38.06 vs. 26.67). While their industry control group peers often default to passive scanning tool administrative habits, these mid-career WiCyS operators bring deep technical precision to the segment.

- **Senior Tier (The Strategic Management Bottleneck):** This technical advantage continues into the senior layer, where WiCyS experts retain a dominant **71.61%** technical capability advantage (52.50 vs. 30.59). Senior WiCyS professionals excel at the deep tactical level, outclassing their benchmark peers in the specific lane of OT Security (52.50 vs. 30.59). However, this technical dominance is held back by a sharp deficit in Leadership Competencies (**-19.10%** deficit). This represents an operational exposure bottleneck: senior technical women in the OT space are kept on factory floors running active engineering defense loops while their male peers are consistently promoted to direct industrial asset budgets, manage vendor contracting, and lead executive critical infrastructure safety councils.

For industrial asset owners, infrastructure operators, and talent strategists, this data provides an actionable path forward. Treating OT security as a simple side task for your corporate IT team creates an immediate operational risk. Sourcing specialized talent through conventional lateral hiring channels is no longer sustainable due to market contraction.

Organizations can build resilient, specialized defense teams by intentionally cross-training female systems engineers, mechanical engineers, and defensive operations specialists in industrial control systems and SCADA protocols. By providing these high-performing junior and mid-career professionals with practical sandbox testing environments and actively breaking down the exposure barriers that prevent senior technical women from taking on corporate budgeting and strategic planning roles, enterprises can secure their physical production environments without disrupting critical uptime or risking operational safety boundaries.

11. Security Architecture & Engineering (SAE)

This functional group typically involves designing and implementing secure information systems for an organization, building defensive engineering infrastructure, and creating security architectures and blueprints that align with risk frameworks—including cloud systems, access control matrices, zero-trust topologies, and cryptographic protocols.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	13	2	6	21
All Others	5	4	7	16

Performance Baseline

The quantitative scoring across all experience levels reveals an exceptional capability advantage for the WiCyS cohort, establishing a commanding Performance Edge in core engineering design, structural blueprinting, and policy translation:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	56.12	38.79	17.33	44.68%
Leadership Competencies	50.09	40.07	10.02	25.02%
Organizational Competencies	58.20	38.84	19.36	49.83%
Professional Competencies	73.75	55.36	18.39	33.21%
Technical Competencies	53.52	36.63	16.89	46.09%

Strategic Analysis

A security blueprint that only lists legacy perimeter firewalls isn't architecture. It's technical debt. Traditional infrastructure engineering routinely fails because it relies on static network perimeters that are completely unsuited for modern, distributed cloud landscapes. When blueprints are drawn without native secure-by-design context, organizations face delayed deployments, broken access dependencies, and fragile configurations that fail under the first sign of an active threat loop.

The macro-level dataset for the Security Architecture & Engineering domain highlights a substantial, aggregate **44.68%** overall Performance Edge favoring the WiCyS population. However, a closer look at the stratified lifecycle data reveals an apparent contradiction that challenges standard workforce planning assumptions. At the mid-career milestone, the WiCyS cohort appears to experience a severe drop, lagging the benchmark control pool by **-45.04%** overall.

Relying on unvalidated resumes or surface-level summaries might lead a CISO to assume a mid-career loss of technical competency. But looking at the participant volume exposes this drop as a clear statistical anomaly rather than a systemic failure: the mid-career WiCyS cohort features a tiny sample size of exactly 2 practitioners. One uncalibrated assessment completely skews the tier.

When we focus on the high-volume tiers where the talent distribution is stable, a major pipeline opportunity becomes clear:

- **Junior Tier (Bypassing Legacy Debt):** The early-career control pool is entering architectural tracks with exceptionally weak baselines (22.88 overall, 20.83 technical). Junior WiCyS practitioners capitalize on this industry baseline failure, securing a stunning **134.99%** overall Performance Edge and a **137.77%** outperformance in core technical execution. Rather than spending months unlearning legacy server structures, these entry-level engineers think natively in zero-trust design. They outclass their peers in key infrastructure components, leading in Access Controls (59.44 vs 21.11, a **180.84%** edge) and Cryptographic Encryption (53.89 vs 10.08, a **434.44%** edge). This group represents an immediate opportunity to fast-track modern cloud-native system design with zero initialization lag.

- **Senior Tier (Structural Engineering Parity):** This modern capability pattern scales effectively into the senior tier, where WiCyS engineering architects re-establish an undeniable **67.53%** overall Performance Edge and a dominant **70.81%** lead in late-career technical profiling (69.45 vs 40.66). These senior leaders maintain absolute control over the tactical layer, showing extensive outperformance in core system defense components: Access Controls (82.50 vs 46.21), Operating Systems Security (80.00 vs 31.85), and Physical Device Security (70.00 vs 32.47).

For workforce planners, the operational takeaway is immediate. Sourcing architecture talent from traditional, hardware-bound control groups leaves your cloud environments exposed. The incoming pipeline of 13 junior WiCyS engineering practitioners represents a highly active resource pool that can be trained in modern system blueprints from the start.

By actively recruiting from this entry-level cohort and deliberately ensuring that mid-career technical women are kept focused on cloud transit routing and systems engineering—rather than being diluted by non-technical project coordination—enterprises can build a resilient, secure-by-design infrastructure that protects digital assets across the entire corporate footprint.

12. Security Assessments/Testing (SAT)

This functional group covers the knowledge, tools, and automated techniques used to identify, scan, and manage system vulnerabilities, configuration drift, and compliance gaps. Unlike advanced offensive simulations, these roles focus heavily on passive reviews, commercial tooling, patch validation, and quality control audits to verify corporate defense baselines.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	14	10	9	33
All Others	6	11	11	28

Performance Baseline

The aggregate performance baseline across all experience levels shows a tightly aligned overall footprint, with the comparison cohort holding minor advantages in administrative and leadership layers, while the WiCyS population secures close technical parity:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	42.64	42.97	-0.33	-0.77%
Leadership Competencies	35.55	40.52	-4.97	-12.26%
Organizational Competencies	41.30	44.89	-3.59	-8.01%
Professional Competencies	69.46	63.16	6.31	9.99%
Technical Competencies	40.69	32.82	0.87	2.17%

Strategic Analysis

Running an automated vulnerability scanner is not a security assessment strategy. It is data processing. Most enterprise workforce leaders confuse tool licensing with risk evaluation, assuming that an analyst who can click “execute” on a commercial platform understands the configuration debt of the network layer. This tactical confusion creates a critical baseline failure: security testing teams produce mountains of raw scan data that engineering teams routinely ignore because it lacks operational context or remediation sequencing.

The quantitative data within the Security Assessments/Testing domain highlights the most clear manifestation of the Confidence-Competence Calibration Paradox observed in this study. In contrast to segments where the WiCyS population enters with high immediate margins, the junior tier data here demonstrates an acute performance deficit, trailing the control baseline by -**56.59%** overall and **-55.33%** in core technical capability (26.85 vs. 60.10).

A targeted skills dissection isolates the exact root cause of this variance:

- **Junior Tier (The Academic Vacuum):** Early-career control group practitioners are highly concentrated in active IT support roles, which gives them a substantial advantage in baseline environment structures. Conversely, over half of the incoming entry-level WiCyS cohort is currently active inside academic pathways, evaluated before entering production networks. These junior candidates suffer from a lack of practical exposure to enterprise release structures. They register minimal capability scores in automated environments, lagging sharply in DevSecOps (11.43 vs. 56.67, a **-79.83%** deficit) and Enterprise Architecture (12.86 vs. 56.67, a **-77.31%** deficit). Because they have only evaluated theoretical infrastructure models, they score poorly in real-world remediation, facing deep gaps in Vulnerabilities Assessment (38.57 vs. 80.00) and Threat Analysis (40.00 vs. 76.67).

- **Mid-Career Tier (The Calibration Transition):** This capability delta represents a temporary dip rather than a permanent lack of skill. As these academically active practitioners cross the bridge into the workforce, their performance metrics enter a steep calibration curve. At the mid-career layer, the technical performance gap begins to close, narrowing from a -55.33% entry-level deficit to **-46.44%** as practitioners gain initial hands-on corporate experience.

- **Senior Tier (The Recovery to Technical Parity):** At the senior layer, this calibration effect reaches maturity. Long-tenured senior WiCyS assessment specialists close the capability distance significantly, rising to a technical score of 52.80 against the benchmark's 63.40 (compressing the gap down to **-16.72%**). They achieve strong alignment in practical infrastructure evaluation, supported by a clear, cross-tier outperformance in professional enablers (**9.99%** aggregate edge) that allows them to communicate risk effectively across corporate teams.

For security executives and talent managers, this profile delivers a clear workforce blueprint. Relying exclusively on self-indicated capability metrics or textbook qualifications for assessment teams leaves organizations vulnerable to major operational blind spots. Academic juniors routinely over-estimate their capabilities because they are isolated from the friction of live corporate networks.

To bridge this gap and maximize talent ROI, enterprise leaders must stop trying to hire fully formed assessment professionals from academic environments. Instead, build structured, lab-based sandbox onboarding models that explicitly focus on cloud-native pipeline integration, continuous deployment tools, and patch management environments. Grounding theoretical concepts in operational reality early fast-tracks time-to-value, transforming analytical thinkers into highly capable technical testing leaders who can successfully maintain your corporate defense perimeters.

13. Software/App Security & Secure DevOps (ASD)

This functional group is responsible for secure coding practices, static and dynamic application security testing (SAST/DAST), securing CI/CD deployment pipelines, automated security control integration, open-source component validation, and managing maturity models across the software development lifecycle (SDLC) to embed security natively within developer workflows.

Demographic

Cohort	Junior-Level	Mid-Career	Senior-Level	Total Participants
WiCyS	14	11	6	31
All Others	6	10	10	26

Performance Baseline

The aggregate performance baseline highlights an apparent baseline gap for the WiCyS cohort, indicating standard historical alignment within traditional software architectures where the comparison pool leverages structured, application-centric career pathways:

	WiCyS	All Others	Difference	Performance Edge
Overall Score	39.50	51.48	-11.98	-23.26%
Leadership Competencies	27.52	48.35	-20.83	-43.08%
Organizational Competencies	36.33	51.25	-14.92	-29.11%
Professional Competencies	69.98	70.85	-0.87	-1.23%
Technical Competencies	38.44	49.53	-11.09	-22.39%

Strategic Analysis

Telling developers to “write secure code” without changing their release tools is a recipe for broken deployments. In application security (AppSec), organizations routinely suffer from a major operational blind spot: treating security as an external inspection step that occurs after software compilation rather than an automated quality control built directly into the CI/CD pipeline. When AppSec teams operate as isolated gatekeepers, they create friction with product development lines, driving up release timelines and causing critical security patches to be delayed.

The quantitative data within the Software/App Security & Secure DevOps domain displays a consistent performance gap, with the control group maintaining an approximate **21% to 23%** overall advantage across the entire career trajectory. This long-term trend shows that the benchmark cohort benefits from established development pathways, particularly within legacy application infrastructure and on-premises release structures.

However, evaluating the data through an objective, skills-first lens reveals that the aggregate deficit obscures a critical core engineering advantage hidden within the pipeline:

- **Junior Tier (The Native Coder Profile)**: Sourcing early-career talent into AppSec requires looking past broad averages. While the junior WiCyS cohort trails by **-22.42%** overall, a deeper look at specific technical capabilities turns this narrative upside down. These entry-level professionals possess strong core coding skills, outperforming their industry baseline peers in Computer Languages (60.83 vs. 44.00, a **38.26%** edge) and Software Development (56.39 vs. 48.00, a **17.48%** edge). Their initial gap is concentrated in high-level governance and deployment structures rather than core programming execution. This means that junior WiCyS talent enters application tracks with the practical engineering skills required to parse source code and write functional scripts immediately, compressing their initialization timeline.

- **Mid-Career Tier (The Transition Bottleneck):** This specific technical strength remains stable at the mid-career layer. Mid-career WiCyS professionals maintain a steady, active pipeline footprint (11 participants vs. 10 for the control pool), representing a viable talent source. However, their technical execution remains isolated from broader release architecture lanes, pointing to a career exposure bottleneck where technical women are kept focused on basic test execution rather than infrastructure scaling.

- **Senior Tier (The Core Developer Engineering Edge):** At the senior layer, the technical outperformance of the WiCyS population becomes clear. Senior WiCyS application engineers outscore their benchmark peers in core technical execution fields, leading in Software Development (76.67 vs. 62.90, a **21.88%** edge) and Operating Systems Security (43.33 vs. 35.24, a **22.97%** edge). The aggregate technical deficit (-16.63%) is driven entirely by administrative and tracking tasks, including severe gaps in Mathematical Reasoning (33.33 vs. 59.42) and Requirements Analysis (56.67 vs. 77.48).

This senior profile demonstrates that late-career technical women in the AppSec space are highly skilled core developers who are currently held back by high administrative burdens and poorly defined product requirements.

For CISOs and application development leaders, this data provides an actionable workforce blueprint. Sourcing AppSec talent from traditional control groups frequently leaves teams reliant on tool managers who can run scan reports but cannot write or refactor code. The incoming pipeline of 25 junior and mid-career WiCyS application security practitioners represents an active, highly capable engineering resource.

To maximize this talent pool, enterprise leaders must deliberately change their team structures. Organizations must transition these highly capable software developers out of routine administrative tasks, manual reporting loops, and abstract compliance requirements. Focus their development explicitly on cloud-native pipeline automation, automated testing tools, and infrastructure-as-code deployments.

By empowering these code-fluent professionals to build automated security controls directly into active developer workflows, enterprises can successfully “shift left,” improving code resilience and eliminating software vulnerabilities before they hit production environments without slowing down product delivery cycles.

About skillrex

Skillrex is a cyber workforce intelligence firm specializing in data-driven capability measurement, benchmarking, and strategic workforce optimization.

Key Offerings & Outcomes:

- **Quantify performance** across roles and experience levels
- **Benchmark capability** against industry baselines
- **Identify gaps** in discrete competencies and skills
- **Design pathways** aligned to business and security strategy
- **Measure improvement** in workforce performance over time

By translating skills data into actionable workforce strategy, skillrex helps enterprises strengthen resilience and operationalize talent development.

As both a Strategic and Research Partner of Women in CyberSecurity (WiCyS), skillrex is proud to support the advancement of a more inclusive, capable, and future-ready cybersecurity workforce advancement of a more inclusive, capable, and future-ready.

Web: skillrex.io
Email: info@skillrex.io

About WiCyS

Women in CyberSecurity (WiCyS) is a nonprofit organization with international reach dedicated to the recruitment, retention and advancement of women in cybersecurity. Founded by Dr. Ambareen Siraj through a National Science Foundation grant given to Tennessee Tech University in 2013, WiCyS offers opportunities, trainings, events, and resources for its community and members.

WiCyS Tier 1 Strategic Partners include: Amazon, Bloomberg LP, Cisco, Ford Motor Company, Google LLC, Microsoft, Palo Alto Networks, SentinelOne, Tenable.

To partner, visit: www.wicys.org/support/strategic-partnerships


skillrex
Cyber Workforce. Delivered.
Women in
CYBERSECURITY
WiCyS