CYBER EXPERTISE AT SCALE

Your Playbook for Scoring an All-Star Team

((CENTRIC))

CentricConsulting.com

CONTENTS

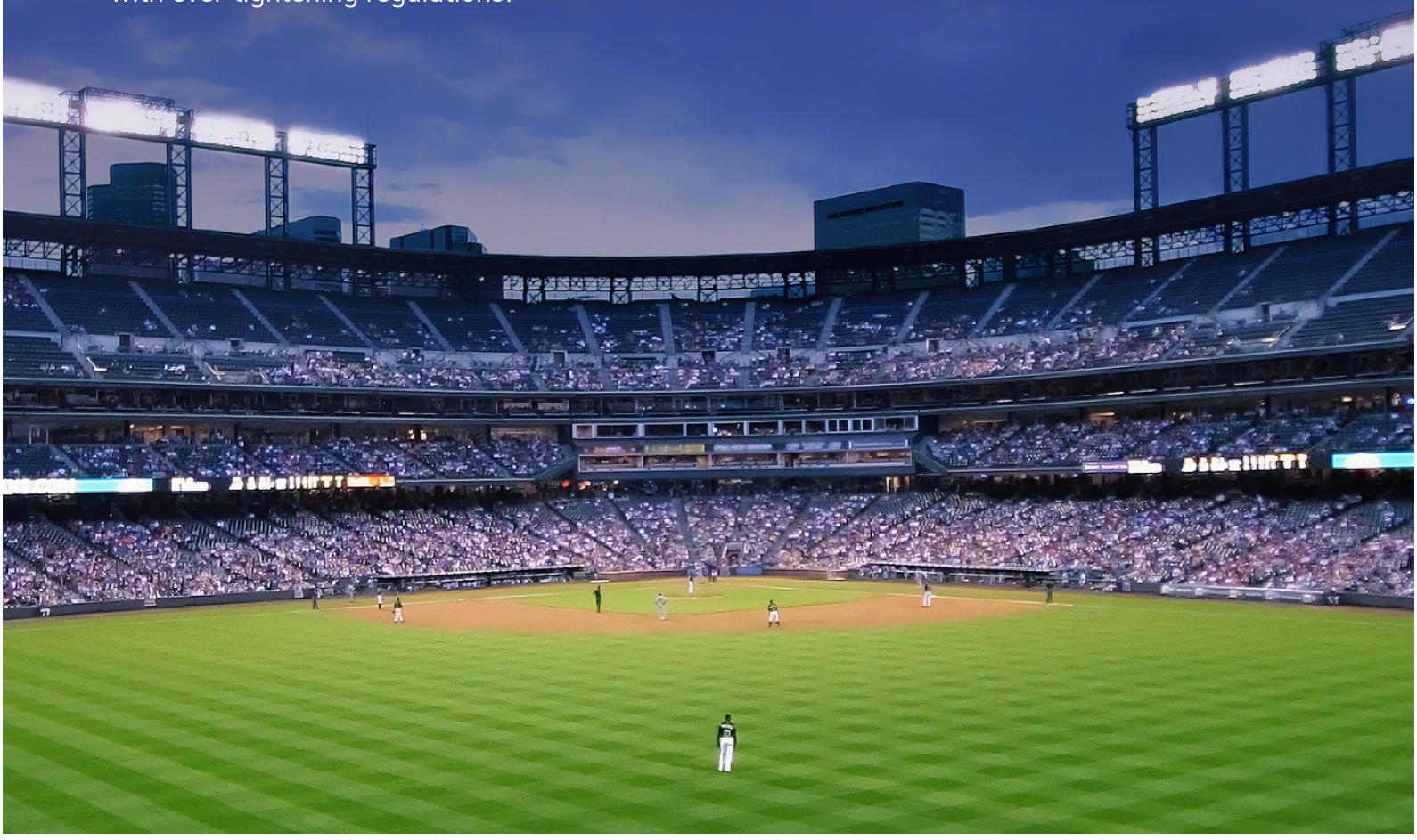
EXECUTIVE SUMMARY

In Cybersecurity, Every Day is Like Game 7 of the World Series

The stakes are sky-high, and the talent to manage those stakes has never been harder to secure.

As cyber threats evolve in complexity, frequency, and regulatory consequences, organizations across industries face a stark dilemma: How do you build a cybersecurity team that's always game-ready without burning out your starters or leaving critical positions unfilled? All while staying compliant with ever-tightening regulations?

Traditional hiring models can't keep up. Static job descriptions, lengthy recruitment timelines, and siloed internal teams often fall short in addressing dynamic and often urgent cybersecurity needs. With critical roles remaining unfilled for months — and burnout rates rising among existing teams — the gap between cyber risk and cyber readiness continues to widen.



This Playbook Offers a **Strategic Path Forward**

Just as winning teams rely on smart scouting, strategic substitutions, and a playbook tailored to each opponent, modern cybersecurity requires a flexible, role-based approach to talent. This guide helps you draft your cyber all-stars, adapt your strategy in real-time, and build a resilient defense capable of withstanding threats both today and in the future.

Here's what you'll learn — and what you'll get:

- A clear view of how the cybersecurity talent shortage impacts organizations like yours and what it means for risk, compliance, and continuity
- Insights into why traditional hiring isn't enough and how flexible models offer a more adaptive solution
- A cybersecurity **self-assessment** framework to evaluate your current strengths, gaps, and future needs
- A comprehensive **role matrix** that outlines the core capabilities needed across security leadership, operations, and compliance
- A build-vs-buy **decision tree** to help you strike the right balance between internal teams and external support
- Trends to watch so you can evolve your talent strategy in lockstep with the threat landscape

In a world where your opponents move fast, your talent strategy must move faster.

This guide provides you with the tools to build cyber resilience at scale, enabling you to protect what matters, meet regulatory demands, and advance your business.

SECTION 1

Outmatched: The Cybersecurity Talent Dilemma

TeamDefense, a fictional financial services company, thought it had time to prepare.

A regulatory deadline loomed ahead, but leadership thought their team would have time to rally. Now, with only weeks to go, there are glaring gaps. Their backlog of critical security tasks continues growing, and it has become painfully clear: Their defensive line — the cybersecurity team — doesn't have the talent or time to fully secure their environment or complete the required documentation.

Recruitment efforts drag. After months, two key roles remain vacant, and qualified candidates are scarce. Meanwhile, the pressure from regulators is mounting, and leadership wants answers, fast.

TeamDefense isn't alone. This is the cybersecurity talent dilemma: High-stakes games happen daily, and there are not enough players on the field.

For many companies, this becomes a turning point: the moment they scramble for someone who can step in quickly, bring the right expertise to the table, and help them meet security and compliance expectations without losing momentum.

Let's take a closer look at what's fueling this growing gap and what it means for businesses trying to keep pace.

The Scale of the Challenge

Like professional sports teams, today's organizations need the right talent in the right positions, ready to respond in real time. But building that lineup has never been harder.

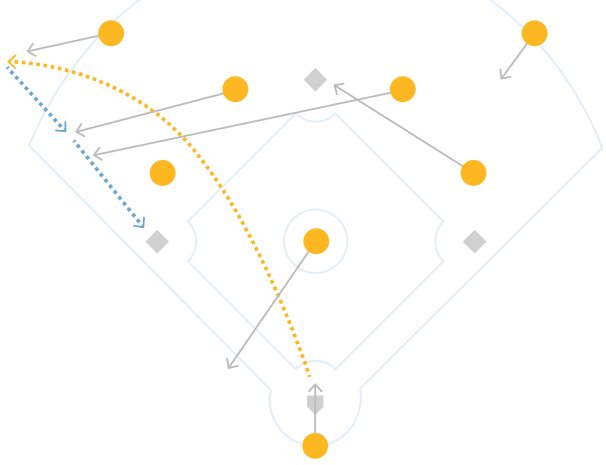
The shortage isn't isolated to one region or sector, either. The World Economic Forum projects the broader global talent shortfall could reach 85 million workers by 2030, potentially resulting in $8.5 trillion in unrealized annual revenue for businesses. For cybersecurity alone, businesses urgently need over four million professionals to close the gap.

Hiring delays make matters worse. Junior roles may fill in one to three months, according to an ISC2 hiring study, but senior-level cybersecurity positions often remain open for six months or more. A Kaspersky survey found that nearly 48 percent of companies require over half a year to find a qualified cybersecurity professional, especially when they require proven experience, compliance knowledge, or niche certifications.

Even once companies fill positions, retention remains a challenge. More than 60 percent of cybersecurity professionals contemplate leaving their current roles within the next 12 months, and only one-third would recommend their employer to others, according to an IANS Research and Artico Search report.

The cybersecurity talent pool isn't deep enough to meet demand.

According to the 2024 ISC2 Cybersecurity Workforce Study, the estimated global cybersecurity workforce stands at 5.45 million professionals. But that's still not enough. The report identifies a global shortfall of 4.76 million additional cybersecurity professionals, meaning that 46 percent of the roles necessary to secure global systems remain unfilled. That workforce gap represents more than a hiring issue. It's a strategic vulnerability.



Why Traditional Hiring Falls Short

Traditional hiring models struggle to meet today's cybersecurity needs, not only in speed, but in specialization, compensation, and flexibility. Like the modern baseball draft, top players demand more — more money, more flexibility, and more tailored roles that fit their skills. Generalists are out. Specialists — whether they focus on cloud security, threat intel, or compliance frameworks — are in.

Recruiting is also limited. Organizations have historically focused on recruiting experienced talent from within cybersecurity or adjacent IT fields. According to the Quarterly Cybersecurity Talent Report from Lightcast, 55 percent of the current cyber workforce came from other cybersecurity or IT roles. Another 38 percent came from non-IT backgrounds with relevant experience. Only seven percent were hired directly after completing their education, with most coming from undergraduate or graduate programs.

This presents a dual challenge: experienced workers remain in limited supply and high demand, while entry-level talent faces significant barriers to entry. That imbalance increases competition and cost, making it harder to build deep and diverse pipelines.

In short, the hiring model most organizations rely on simply isn't fast or adaptable enough to meet the demands of a rapidly evolving threat environment.

Other factors compound the problem:

- **Specialization requirements:** Organizations need deep skills in areas like cloud security, threat intelligence, and regulatory compliance — not generalists.
- **Compensation pressure:** Salaries for cybersecurity roles increased sharply, driven by market competition and internal equity concerns.
- **Geographic constraints:** In-demand professionals may concentrate in specific metro areas or require remote or hybrid flexibility.
- **Time-to-hire lag:** Traditional hiring cycles — from role approval to onboarding — often span months.
- **Retention risks:** In a competitive landscape, even well-paid professionals are frequently courted by other employers or tempted by more flexible roles.

The Business Impact

Cybersecurity isn't just a technical function — it's a strategic capability. And the impact of these talent gaps goes well beyond an empty seat on your team bench. They also delay progress. The inability to fill key cybersecurity roles directly impacts your ability to deliver strategic initiatives, ensure compliance, and protect your customers' and organization's assets.

Here's what's at stake when you're short players:

- **Increased risk exposure:** Understaffed security teams struggle to monitor systems and respond to threats effectively, leading to delays in patching, gaps in detection, and greater vulnerability to breaches.
- **Delayed strategic initiatives:** Without the right expertise, key projects — from cloud migrations to digital product launches — may stall or proceed without adequate security oversight, increasing downstream risk.
- **Rising costs:** To compensate for internal gaps, many organizations turn to consultants or managed security services. Meanwhile, the cost of inaction continues to rise. The average cost of a data breach is $4.76 million globally and over $9.5 million in the U.S. In highly regulated sectors like healthcare and finance, the figure routinely exceeds $10 million per incident.
- **Compliance failures:** Unfilled roles often translate into incomplete security controls, missed audits, and regulatory violations, all of which can result in penalties, reputational damage, and lost partnerships.
- **Board and stakeholder concerns:** As cybersecurity becomes a board-level issue, talent gaps signal deeper operational risk and may lead to increased scrutiny from investors, regulators, and executive leadership.

These aren't simply technical setbacks. They're strategic liabilities. To address these issues, you need to understand the specific expertise your organization needs to stay ahead.

For TeamDefense, the realization that traditional hiring wouldn't close the gap fast enough led them to rethink their approach. They needed a way to align their talent strategy with their risk posture and business priorities, and they needed to do it without losing more time.

In the next section, we'll explore how organizations like TeamDefense can more strategically assess their cybersecurity needs, identify their most critical talent gaps, and draft a strategic cyber roster using flexible talent solutions.

SECTION 2

Scout the Field: Assess Your Cyber Talent Needs

TeamDefense met its compliance deadline, but winning one game doesn't win the championship.

Only weeks later, a wave of international attacks shook their industry. A phishing attempt targeting one of their vendors exposed a blind spot in their defense. In reviewing the incident, they quickly realized they needed two key players on their cyber roster: a seasoned incident response manager and a risk manager — neither of which existed in their current org chart.

As the play unfolded, they uncovered more than immediate gaps. TeamDefense began to see how short-term compliance efforts had masked longer-term weaknesses: They lacked a unified risk strategy, had no escalation playbooks, and their digital transformation roadmap advanced without embedded security review.

In short, the problem wasn't the missing roles. It was the lack of visibility into what they needed in the first place. Their team wasn't built to match the full demands of the game.

This is a scenario we see often. While regulatory pressure is usually the initial catalyst, several common business drivers reveal hidden or emerging talent gaps. Below, we outline six of the most frequent triggers that signal the need for specialized cyber expertise — drawn from real client engagements and industry-wide trends.

01. REGULATORY COMPLIANCE TRIGGERS

New or changing regulations are often the first spark that prompts organizations to reevaluate their security teams. Whether driven by PCI DSS, HIPAA, GDPR or CCPA, compliance requires targeted expertise — not just players who can cover the field, but specialists who know the rules inside and out. From audit readiness and documentation to policy development and technical control implementation, you need these roles to keep regulators from flagging your organization for penalties.

02. DIGITAL TRANSFORMATION INITIATIVES

Modernization efforts, such as migrating infrastructure to the cloud or launching digital platforms, require security by design, not as an afterthought. Too often, organizations treat security like a late-game substitution brought in after they have already migrated infrastructure or deployed products, only to discover critical vulnerabilities that delay launches and increase costs.

A Harvard Business Review article notes that integrating cybersecurity at the design phase avoids costly rework and accelerates delivery. When organizations overlook security early, they often find themselves forced to rebuild systems to meet basic standards for encryption, access control, or data protection.

Case Study

At Centric Consulting, we saw this firsthand when supporting Maas Energy Works, a fast-growing renewable energy provider. The client needed to modernize and scale their operations quickly, but they were also working with sensitive operational data and regulatory requirements tied to energy systems. As they migrated to the Microsoft Cloud, building security into the infrastructure from the start helped ensure identity management, access control, and compliance guardrails were in place — all without slowing down their deployment timeline.

03. INCIDENT RESPONSE AND RECOVERY NEEDS

When an incident hits, it's not merely a test of your systems. It's a test of your bench. In 2024, there were 3,158 recorded data compromises in the U.S. alone, affecting over 1.35 billion individuals. Whether due to a breach, leakage or exposure, these incidents all share one thing in common: sensitive data accessed by unauthorized actors. When this happens, companies need fast, specialized support to contain damage, restore systems, and strengthen controls.

04. STRATEGIC GROWTH AND MERGERS AND ACQUISITIONS

Like trading for new players mid-season, mergers and acquisitions (M&A) often introduces complex challenges. Integrating disparate systems and protocols, aligning organizational policies, and managing culture change all increase your risk. When companies exclude IT and cybersecurity teams from early M&A planning, the result can be costly vulnerabilities post-close.

These integration points require a unified cyber strategy and dedicated roles to ensure infrastructure consolidation, policy harmonization, and secure data transfer. According to a Gartner CEO survey, 85 percent of executives now view cybersecurity as essential to enabling enterprise growth, especially during times of strategic change.

05. LEADERSHIP GAPS AND PROGRAM MATURITY

As your cybersecurity program matures, new leadership roles often emerge. Many organizations recognize the need for a strategic cybersecurity voice at the table — someone who can read the field, translate risk into business language, and align investments with enterprise objectives.

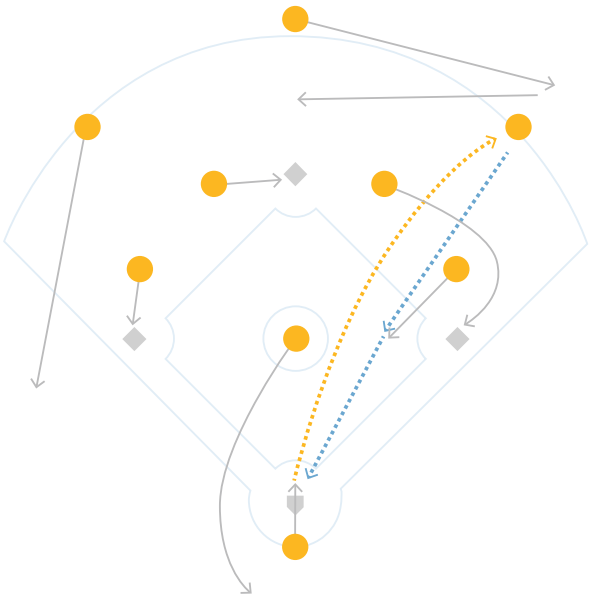
This is especially true after board reviews, major audits, or post-incident assessments, when questions shift from “Are we secure?” to “Are we investing wisely in our security posture?”

06. TECHNICAL IMPLEMENTATION PRESSURE

Sometimes, the playbook is set, but you need the right player to run it. Whether it’s deploying a new endpoint detection platform, building a secure API gateway, or configuring security information and event management (SIEM) tools, implementation bottlenecks often stem from a shortage of skilled engineers.

These gaps can slow or stall technical rollouts, especially when staff lacks experience with specific platforms, cloud configurations, or integration protocols.

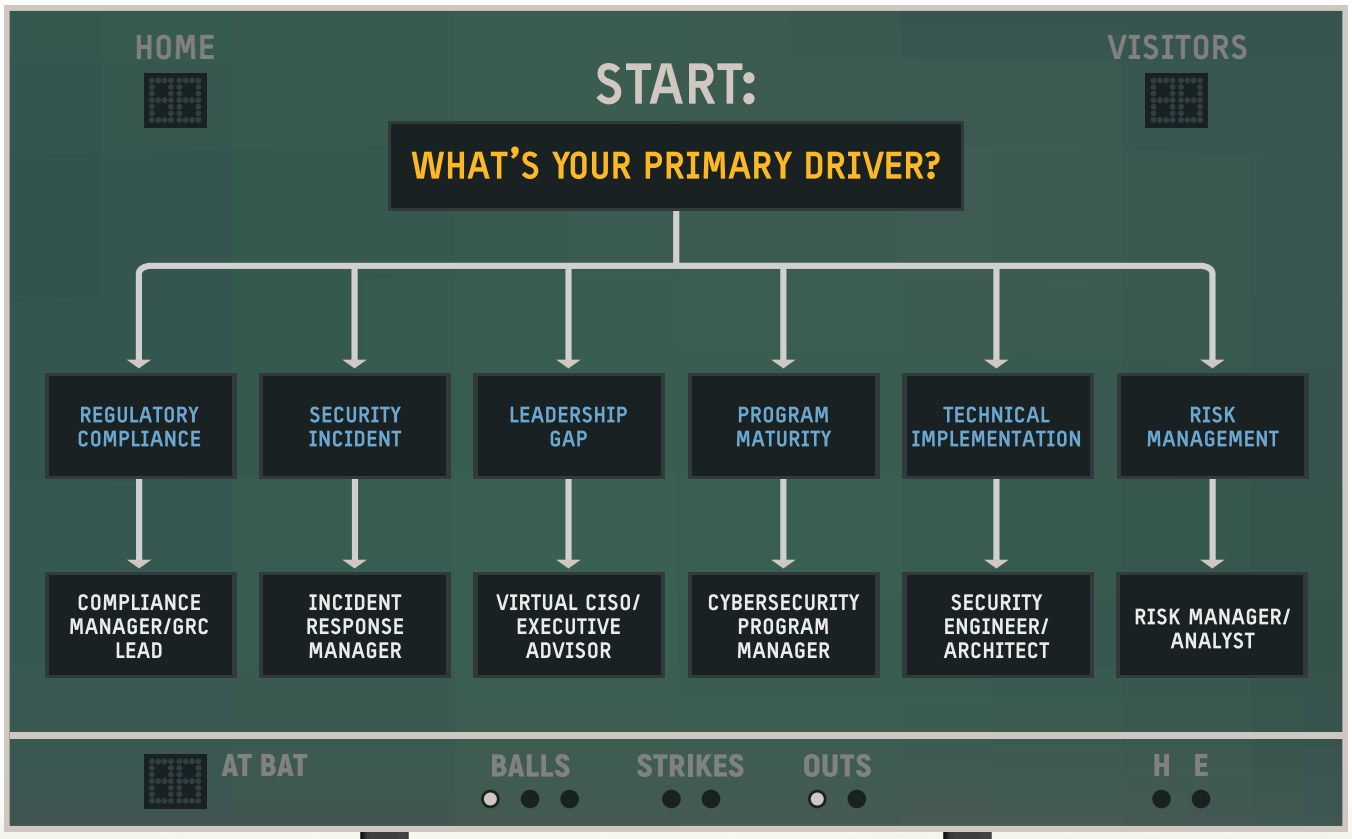
Each of these drivers signals a deeper shift in how organizations must approach cyber talent: not as static roles to fill, but as dynamic capabilities aligned to evolving business needs.



Cyber Talent Needs Assessment Framework

To make this process easier, we have developed a simple decision flowchart that maps common business drivers to the roles most often needed to address them.

Use this framework as a starting point for evaluating your internal gaps or planning future hiring and partnership strategies.



Assess How Critical the Cyber Talent Gap Is

Once you identify what's driving your talent needs, the next step is determining the urgency of the gap. Some needs demand action by halftime. You can address others in the off-season.

For TeamDefense, what began as a high-priority compliance deadline evolved into a broader understanding of their cyber talent needs and a clear realization that not all gaps are created equal. They needed to fill some critical roles immediately, while they could address others through phased planning or external support.

In the next section, we'll introduce a Cyber Expertise Matrix to help you categorize these needs and prioritize them based on urgency and impact.

Use this scale to assess where your organization falls:

HIGH	MEDIUM	LOW
Immediate regulatory deadlines, active breaches, or leadership vacuums	Strategic initiatives, program maturation, or planned implementations	Optimization opportunities, periodic risk assessments, or supplemental support

SECTION 3

Build Your Roster: The Cyber Expertise Matrix

For TeamDefense, the aftermath of the phishing incident was more than a wake-up call — it was a moment of reckoning.

They'd been playing defense without a game plan, scrambling for coverage instead of executing a strategic game plan.

They didn't only need more players. They needed a stronger team strategy.

It wasn't purely about reacting to threats or meeting compliance deadlines anymore. It was about aligning talent to their broader security strategy, prioritizing spend, and gaining clarity on what success looked like. That meant answering new questions: Which roles were truly missing? What outcomes should each role deliver? What kind of engagements made sense given their timeline and budget?

To better understand how to match specific business needs with the right roles, use our Cyber Expertise Matrix. This visual framework helps you:

1. **Identify role needs:** Match your current challenges to “When You Need It” scenarios
2. **Understand deliverables:** Review “What You Get” to align expectations with outcomes
3. **Plan engagement:** Select the right model and duration based on your operating environment
4. **Estimate budget:** Use typical timelines and scope to forecast effort and cost
5. **Define success:** Link deliverables to measurable KPIs like risk reduction, audit readiness, or program scalability

The matrix breaks down four core categories of cybersecurity roles:

- **Leadership & Strategy:** Executive alignment, governance, and communication
- **Program & Governance:** Operational structure, compliance, and control mapping
- **Technical & Implementation:** Tactical deployment and engineering support
- **Specialized Assessment:** Independent analysis, testing, and readiness validation

Each role is organized by:

- **When You Need It:** Key triggers or scenarios
- **What You Get:** Capabilities, responsibilities and outcomes
- **Typical Engagement:** Common delivery models and durations to guide planning

The Cyber Expertise Matrix is designed to simplify your next steps, whether you’re expanding a team, preparing for an audit, or recovering from an incident. The structured framework can help translate urgency into clarity, identifying exactly which positions you need for both short-term compliance and long-term resilience.

Once you identify the right roles and engagement types, the next step is choosing how to source players internally, externally, or both.

Cyber Expertise Matrix

ROLE CATEGORY	SPECIFIC ROLE	WHEN YOU NEED IT	WHAT YOU GET	TYPICAL ENGAGEMENT
Leadership & Strategy	**Virtual CISO (VCISO)**	No security leadership + regulatory pressure, post-breach recovery, board governance requirements	Executive-level strategic planning, risk management, stakeholder communication	6-24+ months, often fractional or interim
	Executive Security Advisor	Board preparation, M&A due diligence, strategic initiative guidance	C-suite counsel, risk translation, strategic alignment	3-12 months, project-based or periodic
Program & Governance	**Cybersecurity Program Manager**	Fragmented security initiatives, program establishment, resource coordination	Comprehensive program governance, roadmap development, control implementation	6-18+ months, part- to full-time
	Compliance Manager	Regulatory deadlines, audit preparation, framework implementation	Deep regulatory expertise, control mapping, audit readiness	3-6+ months, project-based or fractional
	GRC Lead	Governance framework gaps, policy development, risk program maturation	Integrated governance structure, policy frameworks, stakeholder alignment	6-12 months establishment, ongoing oversight
Technical & Implementation	**Security Architect**	Cloud migrations, application modernization, security-by-design initiatives	Secure system design, architecture patterns, technical security guidance	3-12 months, project-based
	Security Engineer	Tool deployments, technical implementations, automation needs	Hands-on implementation, configuration, integration expertise	3-9 months, project-based
	IAM at Scale	Access sprawl, privilege management, Zero-Trust initiatives	Identity architecture, access modeling, life cycle management	6-12 months implementation, ongoing management
Specialized Assessment	**Risk Manager/ Analyst**	Risk program development, strategic decision support, third-party risk	Risk assessment methodology, quantification, treatment planning	6-18 months, often fractional
	Penetration Test Program Manager	Compliance testing requirements, vulnerability program maturation	Comprehensive testing programs, methodology oversight, remediation strategy	3-6 months program establishment
	Incident Response Manager	Active incidents, response preparation, recovery coordination	Crisis management, forensic coordination, stakeholder communication	Days to weeks for incidents, months for program building
	Sourced Internal Audit	Control validation, pre-external audit preparation, independence requirements	Independent assessment, control testing, remediation guidance	1-3 months, periodic

SECTION 4

Balance the Lineup: “Build vs. Buy” Decision Framework

After mapping out their cybersecurity needs and identifying critical roles, TeamDefense faced a familiar and sometimes divisive challenge: How should they fill those roles?

Some leaders wanted to recruit and train their own players, building an internal team that could grow with the organization. Others pushed for external consultants who could hit the ground running. And a third camp proposed a hybrid roster, blending the best of both approaches.

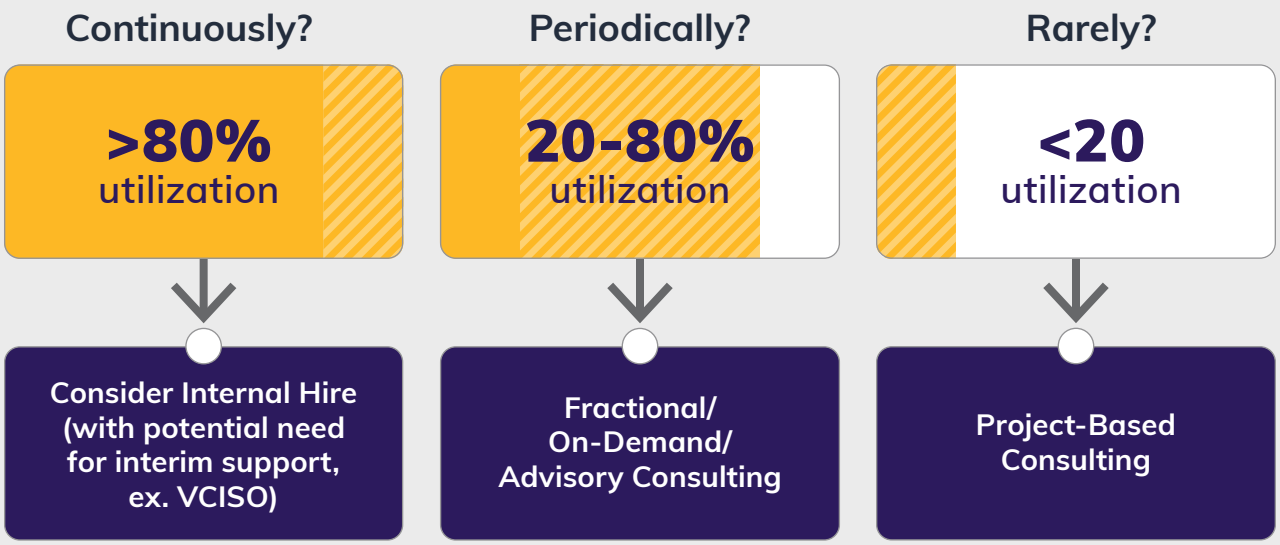
This conversation isn’t unique to TeamDefense. It plays out in nearly every organization at some point in its cybersecurity maturity journey. Fortunately, there are clear frameworks to help you navigate it, starting with one simple but strategic question:

How often does your company need the expertise?

Decision Tree:
Build, Buy or Blend?

Think of each role as your batting lineup. Some hitters you need in every game. Others you only call on when facing a specific opponent or scenario. Use this framework to guide your decision-making around each cybersecurity role you evaluate.

Does your organization need this expertise...



Additional Factors to Consider:

- Can you attract/ retain this expertise locally?
- Do you have the budget for a full-time role + benefits?
- Is this a strategic core competency for your business?
- Can you wait 3-6 months for recruitment and onboarding?

Internal Hiring: When It Makes Sense

Developing talent in-house is like investing in a franchise player — someone who knows your playbook, earns loyalty, and grows with the team. When security is core to your operations — or when you need continuity and embedded decision-making — internal hires offer a sustainable path forward. For organizations with mature programs and sufficient budget, building in-house expertise ensures day-to-day availability and deep integration across teams.

PROS

- Dedicated focus and availability
- Deep organizational knowledge
- Long-term strategic alignment
- Culture integration
- Internal collaboration

CONS

- High total cost (salary, benefits, upskilling, and retention)
- Lengthy recruitment timelines
- Risk of skills becoming obsolete in fast-evolving domains
- Narrower expertise compared to external talent pools

BEST FOR

- Core security operations teams (such as SOC, endpoint, detection, and response)
- Continuous monitoring and compliance support
- Larger organizations with 500 or more employees
- Mature security programs with well-defined architecture and governance

External Expertise: When It Makes Sense

External experts are your free agents — experienced players who bring instant value, especially when time is tight and the stakes are high. When you require speed, specialization or flexibility, external support often makes the most sense. Whether you're facing an audit deadline, navigating a breach, or launching a cloud transformation, outside experts can bring the skills and experience your internal team may not yet have. This model allows you to scale talent quickly and cost-effectively, especially when needs are short-term or narrowly focused.

PROS

- Immediate access to specialized skill sets
- Flexible engagement models (project-based, advisory or fractional)
- Broader experience across industries and platforms
- Cost-effective for short-term or high-skill needs

CONS

- Learning curve within your organizational context and systems
- Limited availability or resource continuity
- Higher hourly rates
- Requires intentional knowledge transfer and documentation

BEST FOR

- Specialized projects like cloud migration and secure app modernization
- Interim leadership needs such as VCISO and M&A due diligence
- Regulatory deadlines or third-party assessments
- Filling gaps while recruiting permanent hires

Hybrid Approach:
The Player/Coach Model

In many cases, the smartest path forward isn't either-or. It's both. By combining internal hires with external experts, you can build sustainable capacity while staying agile enough to address new challenges as they arise.

This approach is especially effective when maturing your security program, balancing short-term and long-term needs, or navigating change without overextending resources.

We describe this as a "player/coach" model where external experts deliver and coach internal staff, enabling knowledge transfer, upskilling, and a smoother handoff of responsibilities over time. Such an approach gives you strategic flexibility, faster time to value, and a more seamless path to sustainable security maturity, especially when internal teams are growing or restructuring.

In scenarios like TeamDefense's, using a structured framework to guide build vs. buy decisions can help align your talent strategy with real business needs. Rather than defaulting to full-time hires or leaning too heavily on outside help, a deliberate approach allows you to allocate resources based on urgency, complexity, and long-term goals.

In the next section, we'll explore how to maximize the value of external engagements, from setting expectations to ensuring outcomes that drive measurable impact.

This flexible mix can look like:

- A core internal team supported by specialized consultants for architecture, testing or compliance
- Ongoing operations handled internally, paired with external advisors to guide governance or board reporting
- Permanent leadership (like a program manager or compliance lead) complemented by project-based experts
- A blend of continuous monitoring with periodic penetration testing or audit readiness assessments

SECTION 5

Get the W: Maximize Value from External Experts

For TeamDefense, bringing in external experts, including a fractional virtual CISO and a security architect, helped address immediate gaps in their cloud modernization effort.

In the same way that signing a free agent doesn't guarantee a championship, simply having outside help wasn't enough.

Their next challenge was to guarantee those engagements delivered more than task completion. They also needed to build internal maturity, strengthen processes, and enable knowledge transfer. These wins drive real transformation — not just checking a box, but leveling up the entire team.

This scenario is common. Many organizations bring in the right external players but fall short when it comes to integration, knowledge retention, and measurable outcomes. The most successful engagements happen when companies treat external professionals as true partners, not one-off vendors. That means providing context, setting expectations early, and planning for knowledge handoff from day one.

To ensure your external engagements deliver lasting impact, focus on four critical practices:

01. CLEAR SCOPE AND STAKEHOLDER ALIGNMENT

Start with a clear game plan. The fastest way to lose momentum is misalignment between internal stakeholders and external partners about their definition of success.

Define business-aligned outcomes. What should this expert accomplish in the next 30, 60, or 90 days? What KPIs or compliance milestones should they prioritize?

For example, are you measuring a reduction in time to detection, or do you want to know how many audit findings your team has remediated? This is especially important in high-pressure situations, such as audits or post-incident recovery, where ambiguity can slow delivery and frustrate everyone involved.

02. SEAMLESS INTEGRATION WITH INTERNAL TEAMS AND PROCESSES

Even an MVP can't win without their team. If consultants operate in a silo, they can't deliver sustained value. Success hinges on how well you embed them into your existing plays — in other words, your workflows, tools, and communication rhythms.

For TeamDefense, embedding the security architect into Agile ceremonies and DevSecOps pipelines could help uncover system-level gaps more quickly and accelerate implementation without duplicating work already in motion.

Looping in external resources early also improves team trust and enables faster decision-making. Instead of "parachuting in," consultants should feel like part of the team, aligned to the mission and the operating tempo.

03. KNOWLEDGE TRANSFER PLANNING THROUGH THE PLAYER/COACH MODEL

Temporary help doesn't mean temporary value. To ensure lasting impact, every external engagement should include intentional knowledge transfer, turning short-term delivery into long-term capability building.

That's why we often recommend a "player/coach" model: external experts don't simply complete work, they mentor your internal team along the way. This approach builds confidence and competence inside your organization, reduces future dependency, and accelerates upskilling, especially in hybrid environments or early-stage security programs.

For example, TeamDefense's virtual CISO could not only lead board-level risk discussions but also coach the newly promoted internal GRC manager on governance models and audit preparation, leaving behind a stronger team rather than merely a finished project.

04. REGULAR PERFORMANCE REVIEWS AND OUTCOME TRACKING

You need to set goals at the beginning of an engagement and track performance along the way. Without defined checkpoints, even experienced players can drift off course or become reactive instead of proactive.

Build in periodic reviews focused on key outcomes, such as audit readiness, time-to-containment, compliance control validation, or maturity progress. For project-based work, define clear milestones and delivery gates to ensure a smooth workflow. For longer-term advisory or fractional roles, assess impact across both tactical and strategic levels. For TeamDefense and others like it, external engagements aren't a short-term fix. They're a catalyst for long-term growth. By clearly defining scope, embedding experts into their teams, and investing in knowledge handoffs, they ensure every consultant leaves behind a more capable and better-aligned security function.

You can do the same. When your external partners are set up for success from day one with shared goals, integrated workflows, and measurable impact, they don't just solve problems. They help your organization raise its game. Your programs mature faster, and your business moves forward with confidence.

In the next section, we'll explore how to future-proof your cyber talent strategy, from emerging trends to building resilience through proactive planning.

SECTION 6

Prepare for Next Season: The Future of Cyber Talent Strategy

With cyber threats growing more sophisticated and regulatory demands intensifying, the race to build scalable and adaptive cyber expertise is just beginning.

Organizations like TeamDefense — and yours — must now look ahead with the same discipline and agility that elite sports franchises apply to roster building. Creating a modern cyber talent strategy means adopting a portfolio approach to resourcing, investing in continuous skills assessment, and remaining open to flexible engagement models.

To future-proof your strategy, it's also critical to strengthen security culture, prioritize team upskilling, and remain responsive to evolving threats like AI-driven attacks. Remote and distributed models will continue to shape how organizations source expertise, while automation and AI will alter the balance between human-led and tool-enabled activities.

Here's how the field is shifting and how you can draft and develop the cyber talent lineup needed to stay in the game.

1 Specialized Skills Are No Longer Optional — They're Foundational

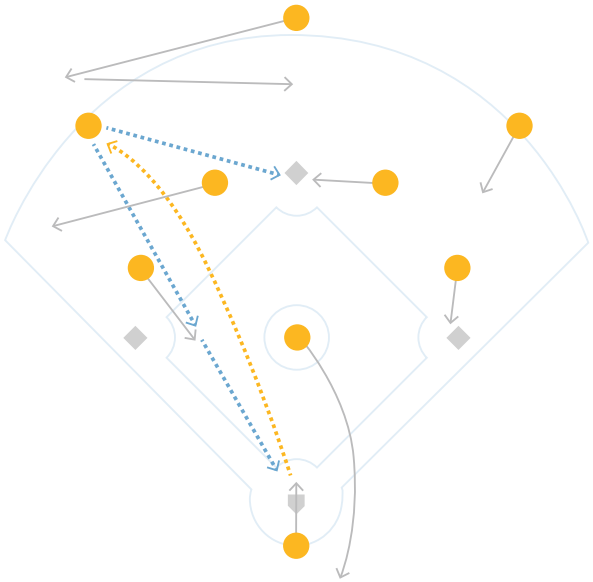
Cyber threats grow more sophisticated by the day. From deepfake-enabled phishing to AI-driven malware, organizations need targeted skills in cloud security, threat intelligence, DevSecOps, and secure software architecture. In fact, according to CompTIA, skills in AI, cloud computing, and cybersecurity are among the most in-demand.

To help, you can build a portfolio-based talent model that balances core hires with specialized contractors. Use regular skills assessments to identify when to upskill internally versus bring in niche expertise. Think of it as knowing when to sub in a closer or bring in a defensive specialist for the final play.

2 Remote and Distributed Talent Is the New Normal

Just as professional teams now scout globally, organizations are expanding their cyber talent search beyond traditional boundaries. Distributed cyber talent allows for round-the-clock coverage and access to hard-to-find skills but requires stronger coordination and integration.

Embrace flexible engagement models, including fractional leadership (such as a virtual CISO), global consultants, and on-demand analysts. Prioritize alignment processes and cultural fit, not only resumes.



3 AI and Automation Are Redefining Job Descriptions

In today's game, AI is both a teammate and an opponent. Roles like prompt engineer, AI threat modeler, and automation architect are emerging, while traditional roles like SOC analyst are evolving.

With IBM reporting that AI proficiency is now among the top five most critical cyber competencies, organizations must review and revise role definitions. They must also upskill current employees on AI tools and supplement them with external advisors familiar with AI implementation in cybersecurity operations.

4 Regulations Are Multiplying and Fragmenting

With overlapping frameworks like NIST, DORA, SEC cyber disclosures, and the EU Cyber Resilience Act, the rulebook is getting thicker and harder to navigate — especially across global operations. That doesn't even touch the number of privacy laws coming online worldwide, from additions to the GDPR to Indonesia's privacy law to all the state-level privacy laws being voted on throughout the U.S.

To navigate these changes, maintain a living compliance map and ensure regular updates. Also, consider retaining GRC experts who specialize in specific geographies or verticals.

Technology alone won't define the future of cybersecurity.

The people you trust to run your plays — the team you develop and the partners you bring in — will define the future of your cybersecurity success.

As threats become more sophisticated and regulatory stakes rise, your talent strategy must be as agile and forward-thinking as your security strategy. Building a resilient mix of internal, external, and hybrid cyber expertise ensures you're prepared not only for today's challenges but also for tomorrow's unknowns.

CONCLUSION

Your Cyber **Championship Strategy Starts Here**

The cybersecurity talent challenge isn't going away, but your approach to tackling it can evolve.

With the right mix of internal hires, external expertise, and flexible engagement models, you can move beyond firefighting and start building true resilience.

The key is moving from reactive talent gaps to a proactive cyber expertise strategy.

Whether responding to an urgent compliance deadline, navigating a breach, or planning long-term program maturity, the strongest companies don't wait until talent gaps slow them down. They make proactive substitutions, call the right plays, and bring in the right players at the right time.

Ready to Build Your Scalable Cyber Expertise Strategy?

Let's discuss your specific situation. Our cybersecurity experts can help you:

- Assess your current gaps and risk exposure
- Design the right mix of internal and external support
- Connect you with vetted specialists matched to your needs
- Develop a right-sized plan for your budget and timeline

Next Steps:

- Schedule a consultation to discuss your cybersecurity talent strategy
- Get a personalized game plan with expert recommendations you can act on
- Explore engagement models aligned to your organizational goals

Schedule Your Strategy Consultation

Don't let talent gaps become security gaps. Let's build your path to cyber resilience together.

CONTACT US

((CENTRIC)) Learn More About Our Services

CentricConsulting.com