Academic & Institutional Programs

Partnership Overview & Reference Guide

About TacRaven Solutions

TacRaven Solutions is founded by U.S. Military Veterans with backgrounds in cybersecurity operations and threat analysis. We work selectively with academic and institutional partners to deliver cybersecurity and digital intelligence education that emphasizes structured analytical thinking techniques and practical cyber operations.

We integrate with your existing frameworks, curricula, and processes, not the other way around. Our engagements are structured, applied, and outcome-driven, designed to complement what you've already built.

Organizations We Work With

Research Universities   R1 and R2 institutions developing cybersecurity and intelligence programs

Community Colleges   Institutions with dedicated cyber or IT security certificate programs

Government Training Centers   Federal, state, and DoD-adjacent workforce development programs

Professional Organizations   Industry associations and credentialing bodies in security and intelligence

Engagement Pathways

01 Academic & Institutional Partnerships

We collaborate with universities and institutions to deliver accredited courses, applied cybersecurity and digital intelligence curriculum, and program-level integration. These partnerships embed rigorous analytical methodology into existing academic structures.

- • Accredited undergraduate and graduate coursework
- • Digital Intelligence & Cybersecurity Foundations
- • APT and threat-actor focused courses
- • Curriculum co-development and program support

Outcome: Students graduate with structured analytical thinking frameworks directly applicable to SOC, threat intelligence, and security analyst roles.

02 Tool-Enabled Training & Assessment

We provide analytical tooling used inside coursework and training environments. Students and professionals evaluate logs, analyze threat behavior, and produce structured assessments using purpose-built platforms. Educational use only: applied analysis, not demonstrations.

- APT log analysis and assessment environments
- Structured analytic workflows
- Assessment-based learning outcomes
- Institutional access (not individual subscriptions)

Outcome: Learners complete hands-on assessments producing analyst-quality deliverables using professional-grade tooling.

03 Advisory & Program Support

We support organizations through advisory work, program design, faculty enablement, and strategic discussions related to cybersecurity and digital intelligence education. These engagements help institutions build and refine their own capabilities.

- Program and curriculum advisory
- Faculty workshops and guest instruction
- Applied threat intelligence briefings
- Strategic education and workforce development support

Outcome: Institutions gain internal capacity to deliver rigorous, analytically-grounded cyber education independently.

Frequently Asked Questions

What is the typical engagement timeline?

Most engagements begin with a 30-minute scoping conversation, followed by a proposal within two weeks. Academic partnerships typically require one semester for curriculum integration. Tool access and advisory engagements can often begin within 4-6 weeks of agreement.

Do we need to change our existing curriculum or systems?

No. We work within your existing frameworks, LMS platforms, and program structures. Our role is to enhance and support what you've already built, not to overhaul it. Whether you're using Canvas, Blackboard, Moodle, or another system, we adapt to your environment and processes.

Can curriculum be customized to our existing program?

Yes. We work with your faculty and program directors to align content with existing learning objectives, accreditation requirements, and student skill levels. Customization ranges from minor adjustments to full co-development of new course material.

Is this compatible with accreditation standards?

Our curriculum aligns with NICE Framework competencies and can be mapped to CAE-CD, ABET, and regional accreditation requirements. We provide documentation to support your accreditation processes as needed.

What does institutional tool access include?

Students and faculty access our analytical platforms through TacRaven Cyber Academy for educational use. We provide institutional partners with monthly performance reports on student progress, plus comprehensive assessments and grades at the conclusion of each course or program. This allows your team to track outcomes without managing the platform directly.

Do you work with government or defense organizations?

Yes. We support federal agencies, DoD-adjacent training programs, and state-level workforce development initiatives. Our founders' backgrounds in military service and cybersecurity operations inform our structured, rigorous approach to these engagements. Specific requirements around security, compliance, or contracting vehicles can be discussed during scoping.

How is this different from commercial training vendors?

We don't sell courses to individuals or run open-enrollment bootcamps. Our focus is institutional: building capability within your organization. We emphasize structured analytical thinking techniques and applied methodology, not commercial certifications repackaged for universities.

What is TacRaven Cyber Academy?

TacRaven Cyber Academy is our internal learning management system where we house and distribute all educational content. Students access course materials and assessments through the Academy. Institutional partners receive monthly performance reports on student progress, as well as comprehensive performance assessments and grades at the conclusion of each course or program.

Consultation Checklist

To help us make the most of our initial conversation, please review the following questions. You don't need formal answers prepared, but thinking through these areas will help us understand your goals and determine the best path forward.

Program Background

- ■ What type of institution are you (university, community college, government, professional org)?
- ■ What program or department would this engagement support?
- ■ How many students or participants would be involved?
- ■ What is the current skill level of your target audience (beginner, intermediate, advanced)?

Goals and Objectives

- ■ What specific outcomes are you hoping to achieve?
- ■ Are there particular skills or competencies you want students to develop?
- ■ Is this engagement tied to any accreditation, certification, or compliance requirements?
- ■ What does success look like for your program?

Current Environment

- What LMS or learning platform do you currently use (Canvas, Blackboard, Moodle, other)?
- Do you have existing cybersecurity or digital intelligence curriculum in place?
- Are there specific tools or platforms students already use?
- What constraints should we be aware of (budget cycles, academic calendars, approval processes)?

Engagement Preferences

- Which engagement pathway interests you most (Academic Partnership, Tool Access, Advisory)?
- What is your ideal timeline for getting started?
- Who else from your organization should be involved in these discussions?
- Are there any specific questions or concerns you want to address in our conversation?

Getting Started

Engagements begin with a simple conversation. No formal RFP required. We'll discuss your goals, explore how we might support your program, and determine if there's a fit. If it makes sense to move forward, we'll handle the complexity so you don't have to.

1. Initial Conversation	30-minute call to understand your goals and program context
2. Proposal & Scoping	Detailed proposal within two weeks, tailored to your needs
3. Engagement Begins	Flexible start based on your academic calendar and timeline

---

Ready to Start a Conversation?

tacraven.com
josh.cellucci@tacraven.com