Cyber Readiness Program for Converged, High-Consequence Environments

Building Operational Capability Across Cloud, SaaS, and Connected Systems

Executive Summary

Modern cybersecurity environments are increasingly complex, yet many organizations remain unprepared to operate during real-world cyber incidents. Despite significant investment in tools, compliance frameworks, and incident response services, organizations often struggle to:

- Reconstruct attacker activity across cloud and hybrid environments
- Correlate evidence across identity, SaaS, and infrastructure systems
- Investigate incidents involving connected operational (OT/IIoT) devices
- Produce defensible, regulator-ready findings
- Operate effectively under pressure

Caduceus Security Group (CSG) addresses this gap by designing and implementing cyber readiness capability—the ability to investigate, respond to, and operate through incidents across converged environments.

The Problem

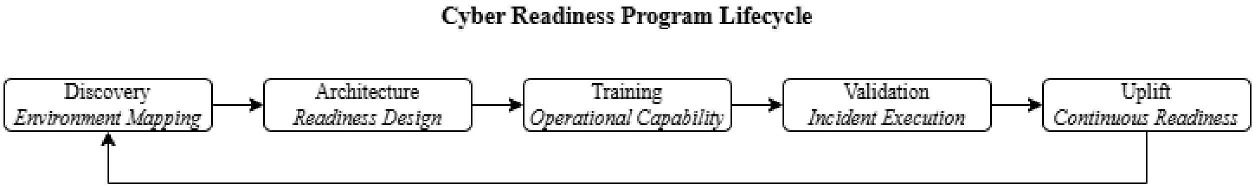
Cybersecurity today faces three systemic challenges:

- **Fragmented environments:** Cloud, identity, SaaS, and OT/IIoT systems are treated as separate domains while attacks move across them seamlessly
- **Tool dependency:** Teams are trained on tools, not investigations, limiting adaptability during real incidents
- **Lack of attribution:** Most approaches stop at what happened, failing to address who, how, and why

Our Approach

CSG delivers a structured Cyber Readiness Program that transforms organizations from reactive to operationally capable. ***We do not deliver quick fixes. We build operational capability***.

Program Structure



1. *Discovery — Environment Mapping*

Identify interdependencies, logging gaps, and forensic blind spots.

2. *Architecture — Readiness Design*

Develop workflows, align telemetry, and design operationally viable architectures.

3. *Training — Operational Capability*

Train teams using real-world artifacts across multi-cloud and SaaS environments, with a focus on end-to-end investigation and attribution.

4. *Validation — Incident Execution*

Validate readiness through real incidents and structured exercises.

5. *Uplift — Continuous Readiness*

Refine telemetry, workflows, and investigative capability over time.

Convergence: Cloud, SaaS, and Operational Technology

Modern environments integrate OT/IIoT with cloud and identity systems, requiring investigations to span multiple domains.

- Evidence often exists outside the originating device
- Identity governs access across environments
- SaaS platforms act as control layers

CSG prepares organizations to operate in these converged environments.

Attribution as an Operational Capability

CSG integrates attribution into investigative workflows, enabling teams to assess behavior, correlate activity across systems, and understand intent.

This approach aligns with broader work in the DFIR community, including practitioners such as Brett Shavers, while extending attribution into operational workflows across converged environments.

What Makes CSG Different

- We build capability, not dependency
- We integrate training with real-world operations
- We address environments as they exist—converged, not isolated

Who We Serve

CSG supports healthcare, financial services, defense, and critical infrastructure organizations operating in regulated, high-consequence environments.

Outcomes

Organizations that complete the Cyber Readiness Program achieve:

- Faster, more accurate incident investigations
- Cross-platform visibility across cloud, SaaS, identity, and OT systems
- Clear, defensible reporting for regulators and leadership
- Reduced reliance on external responders
- Sustainable, long-term cyber capability

About Caduceus Security Group

CSG brings over 26 years of experience in IT and information security, with more than a decade of teaching and developing hands-on training at leading security conferences, including DEF CON, Security BSides, and HOU.SEC.CON.

Our methodology is grounded in real-world forensic practice, using artifact-driven investigations and cyber range environments that replicate modern attack scenarios.

Government & Contracting Information

- Legal Name: Caduceus Security Group LLC
- UEI: SLQDBD3JRFL6
- CAGE Code: 192S0
- NAICS: 541512 (Primary), 541519, 541690, 541611, 611430

Contact for Engagement

Kerry Hazelton
Founder, Principal Consultant
khazelton@caduceussecuritygroup.com