TEAM**ARES**

CRITICAL**START** TEAM**ARES**

The complexity of today's security landscape – combined with an increase in incidents, overall weak security posture and talent shortage – means taking a proactive response to security is more important than ever. Recognizing these challenges, CRITICAL**START**'s TEAM**ARES** stands ready to help organizations prepare for, respond to and resolve breaches by providing offensive red and defensive blue team services.

Our goal is to understand your environment more deeply, to help assess how today's attacks can impact your organization and better defend your environment from potential threats.

RED**TEAM SERVICES**

- **Penetration Testing** including automated and manual penetration tests of internal and external networks to gain access to critical systems or sensitive data. We'll also conduct a compliance penetration test focused on the segmentation of Cardholder Data Environment (CDE) and other requirements set by the PCI DSS compliance rules.

- **Social Engineering** including real-world phishing campaigns to breach a company's network, compromise user credentials, or gain access to data considered sensitive in nature.

- **Physical Penetration Testing** to gain access to secured facilities leveraging multiple techniques such as tailgating, badge access cloning, social engineering, and more.

- **Wireless/Wi-Fi Assessment** to test the security of Wi-Fi networks by attempting to breach a company's wireless network.

- **Web Application Assessment** of clients' web applications through static and dynamic code analysis including a thorough review of application codes, and penetration testing using both automated and manual techniques.

- **SCADA Penetration Testing** to prevent loss of critical infrastructures or life and ensure access to these sensitive environments is locked down and accessible only to those with a valid business need.

- **Password Quality Assessment** to evaluate the current passwords employees and service accounts are using within a network and ensure that password complexity is being enforced to prevent password spraying or guessing attacks.

- **Red Team Training** for a hands-on experience for information security concepts utilized in both offense and defense.

BLUE**TEAM SERVICES**

- **Incident Response (IR) and IR Retainers** provide assurance that when an incident occurs, our expert team stand ready, leveraging our MOBILESOC and comprehensive MDR service to resolve the breach and bring your organization back to business as usual as quickly as possible.

- **IR Plans and Playbooks** to support coordinated response and communications for security incidents.

- **IR Readiness Assessment** to understand the organization's readiness to detect, respond and recover from an incident.

- **Tabletop Exercises** to ensure an organization's IR plan is effective.

- **Compromise Assessments** offer a holistic view of the organization threat landscape.

OUR**TEAM**

CRITICAL**START**'s TEAM**ARES** is comprised of professionals with more than a decade of experience conducting offensive and defensive security services. Our team has expertise in a wide array of industries, including oil and gas, healthcare, app development firms, hospitality, technology, and more.

FOR MORE INFORMATION
Contact us at **criticalstart.com/teamares**