C.L.E.A.R. Philosophy for Cyber Security

Customer Service
Salient CRGT engineers work with customers to develop a full understanding of your priorities, risk tolerance, business requirements, and the impact associated with mission failure. We use this understanding while evaluating threats and in developing a mitigation strategy. Our team carefully evaluates any remediation action with you to ensure success while minimizing the susceptibility to a cyber attack.

One of the most frustrating situations anyone can encounter is a lack of actionable and understandable information. When a critical situation unfolds, you want to know what is going on—without the technical jargon. Our methodology provides information in a transparent and understandable format. We ensure our customers receive, interpret, and are prepared to act on the results, recommendations, and actions being reported by our security professionals.

Leadership
Salient CRGT provides leadership to ensure mission success, reduce risk, and mitigate problems efficiently. It is not enough to only focus on your current Cybersecurity challenge; we minimize risk by anticipating future issues and incorporating them into manageable action plans. We offer a holistic approach to ensure success.

We leverage our Cyber Security Center for Innovation and Growth, working with leaders in the information security arena, to continuously develop innovative solutions for our customers’ evolving challenges. By actively participating in the Cyber Security community, our leaders and engineers are aware of new and unique challenges. This knowledge is incorporated into all aspects of customer interaction, ensuring the best information is available to decision makers and security professionals.
C.L.E.A.R. Philosophy for Cyber Security

Evidence of Success
At Salient CRGT, we acknowledge that without confirmation, IT systems are not secure, regardless of intentions or resources. In all aspects of our cyber security practice, we identify, measure, and report indicators to confirm our successful efforts. We do this through our knowledge of securing, defending, and exploiting networks, along with our extensive experience in software, system, and network design and implementation. We know the information relevant to security professionals; software, system, and network engineers; and executives. We provide a risk analysis and documented metrics in plain language with real benefit throughout the customer’s organization.

Adaptability
Salient CRGT has a history of being an agile company. At a large federal civilian agency we support over 30 programs, in a large-scale, heterogeneous environment spanning the technologies required to meet that agencies cyber security policies, business needs, and regulations. We were chosen to assist this agency in streamlining the migration process of over 500 applications to a secure Linux cloud within a two-year time period, which we did successfully.

Adaptability is critically important in cyber security where the enemy has an asymmetrical advantage. Security is not a static process; it is always changing, requiring continued focus and investment. Salient CRGT revisits strategies that have already been addressed and executed, to determine that the mitigation efforts are still valid and effective. We are dedicated to providing complete protection services to ensure your ongoing operations.

Resources
Effective cyber security is only as good as the resources, Intelligence, and expertise provided to allow mission achievement. We have top cyber resources working in the Department of Defense, the Intelligence community, and federal markets. We have proven methods in critical mission areas and robust technology assets, all which can be applied to securing customer systems.

Our operations staff and program and project managers work with customers to ensure the right mix of skills, personality, and experience are applied to the requirements of each engagement. Our talented staff use their experience and knowledge to adapt to and adopt changing processes and new techniques to respond to today’s constant security challenges. Where appropriate, and without bias, we partner with leading technology vendors to ensure customer needs are met at a reasonable cost.