C.L.E.A.R. Philosophy of Vulnerability Assessments

Salient CRGT engineers have a long history of managing, executing, and refining vulnerability assessments for the DoD and Federal Government. This experience resulted in our C.L.E.A.R. philosophy to vulnerability assessments that focus on customer service to ensure complete, accurate and actionable assessments and remediation activities.

The Salient CRGT C.L.E.A.R. philosophy for cyber security is founded on the premise that mission security and mission success cannot be decoupled and must be complementary. The five principles are:

Customer Service
Leadership
Evidence of Success
Adaptability
Resources

These tenets apply regardless of the Cyber focus or role being fulfilled.

Customer Service

Customer service is the bedrock of our vulnerability assessment approach. We believe that understanding the customer mission and stakeholder needs result in better assessments with realistic mitigation and remediation recommendations. Each assessment begins by assigning an Assessment Team Lead (ATL) responsible for the overall assessment, analysis, reporting and any remediation activities. This ATL works with the customer and other stakeholders to identify and document the scope and boundaries of the assessment including the key operational systems that cannot be affected, as well as establishing the Rules of Engagement (RoE). Agreed upon and understandable RoE minimizes the risks associated with introducing scanning tools and assessment activities into an otherwise stable environment by establishing what tools can and cannot be used and those network or system components which are off limits.

Leadership

Our engineers have been at the forefront of vulnerability assessments for over 15 years. Starting with the first National Security Agency (NSA) Information Assurance Methodology (IAM) courses in 1998 through today's advanced assessment techniques and technology, our engineers are battle tested and highly experienced. We continue to push the envelope in how to assess, manage and remediate wireless, mobile and Bring Your Own Device (BYOD) vulnerabilities of today's workforce. Our participation and support across the cyber operations community provides a distinctive view of vulnerabilities, attack vectors and mitigations necessary to secure our customers most critical assets. We leverage our Cyber Security Center for Innovation and Growth, as they work with leaders in the information security arena, to develop innovative solutions to address our customers' evolving assessment challenges.

Evidence of Success

Metrics are an important measure of how successful a vulnerability assessment is and its value to an organization. We have developed several metrics that we feel provide an accurate representation of the success and utility of our assessments. First, as part of our initial assessment meetings, we provide the customer with pre-assessment findings based on the systems, customer, and operational environment and allow the customer to review and mitigate any of our "Most Common Vulnerabilities" for the given system or network. As we progress through the assessment, we provide intermediate findings for any activities that are critical to the well-being of the systems that are being assessed. After the assessment, we provide a "Before and After" threat picture to show how and where our recommendations improved security. Finally, for previously assessed systems, we provide a list of findings showing recommendations that were not implemented or have been reintroduced by new systems or changes to the network enterprise.

SalientCRGT

SalientCRGT.com
4000 Legato Road • Suite 600 • Fairfax, VA 22033 • 703-891-8200

C.L.E.A.R. Philosophy of Vulnerability Assessments

Adaptability

Our vulnerability assessment approach adapts to infrastructure changes, new threats, and vulnerabilities throughout the assessment. It is critical to a successful assessment to incorporate new and changing information throughout to ensure a complete assessment and minimize risk during the assessment. We incorporate incremental reporting to ensure critical vulnerabilities are identified with recommended mitigation actions and reported to decision makers and systems engineers quickly and effectively. Incremental reporting and constant monitoring of zero-day and new vulnerabilities ensure a complete vulnerability picture at the time of completion.

Resources

Effective use of limited resources is critical in today's IT environment. At Salient CRGT, we understand that criticality and have adapted the four-phased industry best practice to ensure efficient use of vulnerability and mitigation resources.

Phase 1 Planning	**Phase 2** Discovery	**Phase 3** Assessment	**Phase 4** Reporting
Analysis			
Incremental Reporting			

Phase 1 – Planning: Salient CRGT initializes assessments, formalizes agreements, and establishes the project schedule and deliverables including: point of contact (POC) coordination, mission impact, Rules of Engagement, and scope development for the specific assessment.

Phase 2 – Discovery: This phase is critical to ensure the assessment meets the needs of the customer by identifying pertinent assets through technical and non-technical enumeration and document review. Discovery provides the assessment team and customers a clear and full picture of what is to be assessed by developing a network map and initial threat picture of the systems being assessed.

Phase 3 – Assessment: Salient CRGT performs and validates scans. We verify information collected in the discovery phase and we collect host/system information for tabletop and detailed analysis. We may then use the results to update documentation, system security plans, and certification test plans to proactively identify discrepancies as well as validate adherence to approved security-relevant changes.

Phase 4 – Reporting: During the Reporting Phase, Salient CRGT reviews the recommendations and works with site personnel to establish a mitigation/remediation strategy. We coordinate the Plan of Action and Milestones to resolve identified issues. At this point, the Vulnerability Assessment Program (VAP) team works with the designated customer support team to incorporate proactive standard operating procedures (SOPs) into their internal processes and contract support agreements.

Analysis plays a vital role in identifying potential risks at and within every phase. At Salient CRGT, we provide immediate customer notification upon discovery of a problem or a potential or existing threats, and move forward to develop and confirm a proposed mitigation method. This reduces liability and the risk profile by remediating vulnerabilities as soon as is prudent.

SalientCRGT

SalientCRGT.com
4000 Legato Road • Suite 600 • Fairfax, VA 22033 • 703-891-8200