Cybersecurity

Life Cycle Engineering's Cybersecurity Focus Areas

Cybersecurity Development – LCE team members have the skills and experience to create and maintain system security at any point in the software creation process, helping to keep your organization's systems and information secure. We tailor our role to your organization's needs, including roles like these:

- Providing engineering designs for new software
- Leading software design, implementation and testing
- Creating secure software tools and systems
- Developing and implementing a software security strategy
- Performing on-going security testing for software vulnerabilities
- Advising team members on secure programming practices
- Researching and identifying flaws, then fixing mistakes
- Troubleshooting and debugging issues that arise
- Maintaining technical documentation

Cyber Operations - LCE's experts understand the entire scope of cyberspace and related operations, both technical and non-technical. This means we can guide you in issues related to computer architecture, programming, data structures, networks, internet, database systems, information assurance, cryptography, and forensics. The technical aspects are balanced with areas such as policy, law, ethics, and social engineering.

Computer Network Defense and Offense - To protect your network against infiltrations resulting in service/network denial, degradation and disruptions, we can establish processes and protective measures that use computer networks to detect, monitor, protect, analyze, defend, and attack.

Identity Management - We can help you create a secure identity management system that manages the roles and access privileges of individual network users within a system, such as a company, a network, or even a country.

Continuous Monitoring - To monitor network traffic for security attacks or intrusions, our experts use tools such as HBSS and Snort; to scan systems for vulnerabilities they use tools such as ACAS and Retina.

Cybersecurity Architecture - Our experts design security architecture to address the potential risks involved in a certain scenario or environment. The architecture specifies when and where to apply security controls. Design principles are reported clearly, and in-depth security control specifications are generally documented in independent documents.

Computer Security Awareness and Training - We provide training in security best practices principles to employees to help reduce individual security breaches or incidents. LCE currently provides training through the Institute RMF and Hack Warz® classes.

Critical Infrastructure Protection - We can design, implement and monitor security on SCADA and industrial control systems. LCE has past performance in this area with PIT systems for the U.S. Navy.

Policy and Compliance - LCE can create policy and compliance documents, which are typically very specific to a project or organization. LCE has extensive experience in this area, especially in policy compliance and creating policy documents for NSWCPD.

Security Hardening - We apply security best practices to servers, networks, and systems, following the DISA-provided security implementation guides (STIGs) and NIST SP 800 series security guidelines. For the last 10+ years, LCE has provided security hardening services for many customers and/projects, including NCES, PEO ES, PEO GES, JEOD, DDESB, and Forge.mil.

System Certification and Accreditation (DIACAP) / Risk Management Framework (RMF) - We create artifacts and accreditation/authorization packages for projects to receive authorization to operate (ATO) on DoD networks. LCE has extensive experience in supporting customers in C&A/A&A, having created more than 100 packages for accreditation. Customers supported include NSWCPD Code 104 and Dept 50, DDESB, Forge.mil.

Cybersecurity

Cybersecurity Framework Functional Areas

Establishing and maintaining cybersecurity requires strategically developing these five functions:

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.