**LECS REFERENCE, COMPLIANCE AND CERTIFICATION SUPPORT TABLE**
**Q1/2022**

## NIST SP800-171

NIST SP800-171 is a codification of the requirements that any non-federal computer system must follow in order to store, process, or transmit Controlled Unclassified Information (CUI) or provide security protection for such systems. This set of guidelines imposes administrative and technical requirements on contractors and subcontractors of federal agencies that store, transmit, or manage CUI. This document is based on the Federal Information Security Management Act of 2002 (FISMA) Moderate level requirements. It went into full effect on December 31, 2017.

| CATEGORY | SUBCATEGORY | LECS TECHNOLOGY or LECS SOC Service | HOW IT HELP |
|---|---|---|---|
| 3.3.1 | 1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. | LECS SOC Service | LECS SOC Service provides software and hardware necessary to comply with security policy.<br>LECS device/SaaS, in the specific case, can monitor the network data flow to find any anomalies or security risks it may encounter. Also, the service implements high human-skill in cybersecurity to provide the correct implementation of security policy. |
| 3.6.1 | Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. | | |
| 3.11.1 | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI | | The Security service provide a specific security operations, as vulnerability assessment, penetration testing, OSINT Gathering, Dark Web gathering and many more related security service, Response plan and risk analysis included. |

| | | | |
|---|---|---|---|
| 3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. | Service Assessment | |
| 3.11.3 | Remediate vulnerabilities in accordance with risk assessments.information in systems and applications. | | |
| 3.12.2 | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems | | |
| 3.13.1 | Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems | LECS<br>LECS +<br>LECS 4.0<br>LECS SaaS<br>LECS SOC Service | The LECS device has an engine that constantly monitors the traffic it encounters and works to detect network malware and infections that are proliferating.<br>It also performs a myriad of data stream analyzes, exploits, shellcodes, and more.<br>LECS generates a security LOG, classified for risk, ready to analyze for a SOC Service. |
| 3.14.2 | Provide protection from malicious code at designated locations within organizational systems. | | |
| 3.14.3 | Monitor system security alerts and advisories and take action in response. | | |
| 3.14.4 | Update malicious code protection mechanisms when new releases are available. | LECS<br>LECS +<br>LECS 4.0<br>LECS SaaS | Tiresia engine provides cloud support with ML engine to preview and mitigate the network threat.<br>Automatic updates also, optimized on customer needs, improve the detection. |
| 3.14.6 | Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and | LECS<br>LECS + | The LECS device has an engine that constantly monitors the traffic it encounters and works to detect network |

| | | | |
|---|---|---|---|
| | indicators of potential attacks | LECS 4.0<br>LECS SaaS<br>LECS SOC Service | malware and infections that are proliferating. It also performs a myriad of data stream analyzes, exploits, shellcodes, and more. LECS generates a security LOG, classified for risk, ready to analyze for a SOC Service. |
| 3.14.7 | Identify unauthorized use of organizational systems | | |