LECS REFERENCE, COMPLIANCE AND CERTIFICATION SUPPORT TABLE
Q1/2022

NIST V1.1

The U.S. Commerce Department's National Institute of Standards and Technology (NIST) has released version 1.1 of its popular Framework for Improving Critical Infrastructure Cybersecurity, more widely known as the Cybersecurity Framework. The framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. It was developed with a focus on industries vital to national and economic security, including energy, banking, communications, and the defense industrial base. It has since proven flexible enough to be adopted voluntarily by large and small companies and organizations across all industry sectors, as well as by federal, state, and local governments

CATEGORY	SUBCATEGORY	LECS TECHNOLOGY or LECS SOC Service	HOW IT HELP
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.	PR.AT-1: All users are informed and trained	Service training	The Training service provide 3 level of training, based on the specific final user. From anti-phishing technique, to advanced policy for sys admin.
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood	DE.AE-2: Detected events are analyzed to understand attack targets and methods	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	Specto engine of LECS Technology provide a solid engine for threat and anomaly detection. Automatically apply a classification based on varius level. The LECS device has an engine that constantly monitors the traffic it encounters, and works to detect network malware and infections that are proliferating. The SOC Service adds further human-skill review and analysis of LECS LOG and many more.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors.		
	DE.AE-4: Impact of events is determined.		

Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures	DE.CM-1: The network is monitored to detect potential cybersecurity events.	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	LECS SOC Service provides software and hardware necessary to comply with security policy. LECS device/SaaS, in the specific case, can monitor the network data flow to find any anomalies or security risks it may encounter.
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events		
	DE.CM-5: Unauthorized mobile code is Detected		
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.		
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-5: Detection processes are continuously improved.	LECS LECS + LECS 4.0 LECS SaaS LECS SOC Service	Operation as backup redundancy, or policy implementing are integrated in all services. Also, the Tiresia engine provides cloud support with ML engine to preview and mitigate the network threat. Automatic updates also, optimized on customer needs, improve the detection.
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	RS.RP-1: Response plan is executed during or after an incident.	LECS SOC Service	SOC Service provides a specific response plan, based on assets and needs of the company or Government.
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	RS.CO-2: Incidents are reported consistent with established criteria		

Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	RS.AN-1: Notifications from detection systems are investigated. RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers).	LECS SOC Service	The SOC Service adds further human-skill review and analysis of LECS LOG and many more. Also, the LECS and other managed devices have been updated based on last threat disclosure. Tiresia engine, for example, actively supports this operation.
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained. RS.MI-2: Incidents are mitigated.	LECS LECS + LECS 4.0 LECS SaaS	The LECS device automatically responds to isolate the threat in an air-gap way. This patent technology provides an energetic mitigation of the threat.
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities	RS.IM-1: Response plans incorporate lessons learned.	LECS SOC Service	The SOC service and the LECS device together provide an optimal component in user defense-chain. Operation as backup redundancy, or policy implementing are integrated in all services. Also, the Tiresia engine provides cloud support with ML engine to preview and mitigate the network threat.