Cybersecurity consultations

Lighthouse Labs Graduates will conduct a number of scans and investigate your company's cybersecurity infrastructure, to prepare a report that will help you proactively identify and address potential security weaknesses within your digital infrastructure.

This in turn helps prevent costly data breaches, downtime, and reputational damage, while also demonstrating a commitment to safeguarding sensitive information, and enhancing trust with customers and partners.

Below are three sample formats for assessments and the resulting reports produced by our Cyber grads.

1. Vulnerability assessment report and recommendations format:

- **Executive summary:** A short summarization of the assessment that was carried out and why, what results were found, and an overview of the end recommendations you are proposing.
- **Scan results:** A detailed explanation of the results from the scan, how the results have been categorized, and how the vulnerabilities are ordered.
- **Methodology:** The tools and tests used, purposes for each scan, tool, and test, and what environment each tool was used in.
- **Findings:** The description of the systems scanned successfully or not and why.
- **Risk assessment:** The index of all vulnerabilities found, categorized as Critical, High, Medium, or Low severity, explanations of risk categories, list of all vulnerabilities with details on vulnerable target/service/software, etc., description, solution, and how many are affected.
- **Recommendations:** The full list of actions that should be taken in prioritized order with explanations on why they recommend the order and recommendations on security policies, and configurations.

Alternate format: Video presentation of the vulnerability assessment report and recommendations

- Five-minute video presentation giving an overview of the executive summary for the report tailored for an executive-level audience.
- Presentation of findings and recommendations as a slideshow with voiceover.

2. Security architecture overview and recommendations:

- **Introduction:** Purpose of the report and its scope, including any limitations in the assessment.
- **Current security landscape:** Details of the existing security architecture, vulnerabilities, and risks identified during the assessment.
- **Security architecture goals:** Outline of the business requirements, compliance considerations, and future growth plans that influence the security architecture recommendations.
- **Security architecture recommendations:** Detailed recommendations for various security domains, including network security, data security, endpoint security, IAM, cloud security, incident response, and physical security.
- **Implementation strategy:** Proposed phased approach to implementing the recommended security measures, including resource requirements and timelines.
- **Conclusion:** Summary of the key findings with a focus on the importance of implementing the security architecture recommendations.

3. Investigation & research report:

Investigation and research report on a cybersecurity attack

- Identification of the victims of the attacks
- Description of technologies and tools used in the attack (stolen data, ransom, system damage, etc.)
- When the attack happened within the network
- List of all systems targeted
- Motivation of the attackers in this case
- Outcome of the attack (stolen data, ransom, system damage, etc.)
- Recommended mitigation technique to prevent these attacks in the future
- Description of security controls that would help mitigate these risks.