The objective of an API security program is to protect APIs (Application Programming Interfaces) from various threats and vulnerabilities, ensuring the confidentiality, integrity, and availability of data and services exposed through APIs. Here are the primary objectives of an API security program:

1. **Protect Data**: Safeguard sensitive data transmitted over APIs from unauthorized access, disclosure, and tampering. Ensure that only authorized users or applications can access and manipulate data through APIs.
2. **Prevent Unauthorized Access**: Authenticate and authorize clients accessing APIs to ensure that only authenticated and authorized users or applications can interact with API resources. Enforce access controls to restrict access to sensitive data and functionality based on user permissions and roles.
3. **Mitigate Security Threats**: Identify and mitigate common API security threats such as injection attacks, broken authentication, improper access control, insecure deserialization, and sensitive data exposure. Implement security controls and best practices to minimize the risk of security breaches and attacks.
4. **Ensure Compliance**: Ensure compliance with industry regulations, standards, and privacy laws governing the protection of sensitive data and personal information transmitted over APIs. Implement security measures and controls to meet compliance requirements and mitigate legal and regulatory risks.
5. **Maintain Availability**: Ensure the availability and reliability of API services by protecting against denial-of-service (DoS) attacks, excessive API usage, and other threats that could disrupt API operations and impact business continuity.
6. **Build Trust**: Build trust with API consumers and stakeholders by demonstrating a commitment to security and privacy. Provide assurances that APIs are secure, reliable, and compliant with industry best practices and standards.
7. **Support Business Goals**: Enable the secure and seamless integration of applications, systems, and services through APIs to support business objectives such as digital transformation, innovation, and collaboration. Ensure that API security efforts align with business goals and contribute to the organization's success.
8. **Detect and Respond to Security Incidents**: Establish monitoring, logging, and incident response capabilities to detect and respond to security incidents in a timely manner. Implement security controls and processes to detect anomalous behavior, investigate security events, and mitigate security incidents effectively.
9. **Enable Secure Development Practices**: Promote secure coding practices and provide training and awareness programs for developers to educate them about API security risks and best practices. Integrate security into the software development lifecycle (SDLC) to ensure that security is considered at every stage of API development.

10. **Continuous Improvement**: Continuously assess, monitor, and improve the effectiveness of API security controls and processes. Stay informed about emerging threats, vulnerabilities, and security trends to adapt and enhance the API security program over time.

By achieving these objectives, an API security program helps organizations mitigate risks, protect sensitive data, comply with regulations, and build trust with stakeholders, ultimately supporting the secure and reliable operation of APIs and the underlying systems and services they expose.