Botium Toys: Audit scope and goals

Summary: Perform an audit of Botium Toys' cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as "high risk," and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Scope: The scope of the audit includes the following systems: accounting, end point detection, firewalls, intrusion detection system, and SIEM tool. These systems will be assessed based on current user permissions, implemented controls, and procedures and protocols. It is important to ensure that the existing user permissions, controls, procedures, and protocols comply with PCI DSS and GDPR requirements. Additionally, the audit will account for both hardware and system access in terms of current technology.

Botium Toys internal IT audit will assess the following:

- Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
- Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
- Ensure current technology is accounted for. Both hardware and system access.

Goals: The objectives of the audit encompass several key areas. First and foremost, we aim to achieve strict adherence to the NIST Cybersecurity Framework (CSF). In addition, our goal is to establish a comprehensive and compliant process that effectively safeguards our systems. To enhance our overall security posture, we will focus on strengthening system controls, implementing the least privilege concept to manage user credentials securely. Moreover, we will actively develop and implement robust policies, including playbooks, to guide our cybersecurity practices. Ultimately, our objective is to ensure that we meet all relevant compliance requirements, demonstrating our commitment to maintaining a secure and resilient environment.

The goals for Botium Toys' internal IT audit are:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements