Cybersecurity Capstone Case Study

Botium Toys Cybersecurity & Risk Management Program

Background

Company: Botium Toys

Industry: Retail / e-commerce

Challenge: Rapid growth led to new IT systems, online payments, and global customer data storage. Security and compliance gaps emerged (PCI DSS, GDPR, SOC2).

Goal: Build a comprehensive cybersecurity program that addresses governance, risk, detection/response, and technical hardening.

Governance & Risk (GRC)

Projects Applied:

- - Risk Assessment Report
- - Risk Register
- - Vulnerability Assessment
- - PASTA Threat Modeling
- - Security Policy Drafts
- - Access Control Worksheet
- - Data Leak Worksheet
- - Controls & Compliance Checklist
- - Botium Toys Risk Assessment

Findings:

- - Weak access control, broad permissions, missing RBAC, insider risk
- - Data leaks possible due to missing encryption
- - PCI DSS & GDPR controls incomplete (logging gaps, missing IR plan, untested DRP)

Recommendations:

- - Implement RBAC + MFA

- - Encrypt customer data
- - Establish compliance program
- - Update policies, train staff

Incident Response & Forensics

Projects Applied:

- - Incident Report Analysis (DDoS)
- - Network Traffic Analysis
- - Incident Response Playbooks
- - Final Breach Report

Findings:

- - E-commerce vulnerable to forced browsing (led to PII breach)
- - SOC flagged phishing attempts
- - Network analysis revealed ICMP floods & DNS anomalies

Response:

- - Contained DDoS
- - Isolated compromised systems
- - Reset credentials
- - Notified customers
- - Introduced IR playbooks for phishing, ransomware, insider threats

SOC / SIEM Investigation

Projects Applied:

- - Splunk SIEM Log Analysis Project
- - Alert Ticket – Phishing Escalation

Findings:

- - Splunk detected brute-force attempts (svc_backup from Brazil)
- - Credential stuffing (jdoe from Russia)

- - Impossible travel (asmith US→DE)

Actions:

- - Blocklisted malicious IPs
- - Enforced MFA
- - Created Splunk dashboards (failed IPs, failed→success, impossible travel)

Systems Hardening & Automation

Projects Applied:

- - Linux File Permissions
- - Python Automation (IP allow list)
- - SQL Log Queries

Actions:

- - Restricted Linux servers with least privilege
- - Automated IP allow list cleanup with Python
- - Queried SQL logs for anomalous logins

Professional Development & Strategy

Projects Applied:

- - Security Organization Worksheet
- - Controls & Compliance Checklist

Actions:

- - Mapped to ISC2/ISACA/CSA frameworks
- - Identified certifications (CISSP, CISM, CCSK)
- - Strengthened PCI DSS/GDPR/SOC2 readiness

Outcome & Impact

- - Reduced insider/data leak risk with RBAC + encryption
- - Improved detection with Splunk dashboards & alert tickets

- - Cut incident response time via playbooks
- - Strengthened compliance for PCI DSS, GDPR, SOC2
- - Enabled proactive defense with automation & log analysis

Capstone Value

This case study ties together all projects into a unified cybersecurity program.

It demonstrates the ability to:

- - Assess risk (governance & compliance)
- - Detect & investigate (Splunk, network forensics, SQL)
- - Respond & recover (IR playbooks, reports, automation)
- - Align with compliance (PCI DSS, GDPR, SOC)