Securing Twitch: A CISSP-Based Cybersecurity Strategy

Group 8
Rochan Aminzadeh (2130140)
Abdullah Bhatti (2122427)
Vito Mkrtychyan (2222582)
Dennis Nazarchuk (2320352)
Aqdas Tanweer (2320136)

B BUS 489 - Anurag Tewari
06/12/2025

[2] Executive Summary

Project Title:
Securing Twitch: A CISSP-Based Cybersecurity Strategy to Mitigate Risk, Strengthen Access Controls, and Ensure Platform Integrity

Twitch is one of the world's largest live-streaming platforms, enabling millions of users to watch, create, and monetize content in real time. However, its size and complexity also make it a high-profile cybersecurity target. In 2021, Twitch experienced a major data breach that exposed internal tools, source code, and confidential creator earnings. Combined with frequent DDoS attacks, ongoing AutoMod criticism, and weak account protections, these incidents exposed critical vulnerabilities in Twitch's cybersecurity infrastructure.

The objective of our capstone project was to apply the CISSP framework to address these issues systematically. Our goals included strengthening Twitch's Identity and Access Management (IAM), developing a CISSP-aligned Incident Response (IR) Plan, evaluating AI moderation risks, and delivering clear, actionable security recommendations.

Using CISSP principles—particularly in Security & Risk Management, Security Operations, and Identity & Access Management—we identified four primary risks: excessive admin privileges, lack of AI transparency, poor DDoS mitigation, and limited user education on security.

Key deliverables included an enhanced IAM role table, a structured IR plan, a security architecture model, and an end user security guide. Our final recommendations focus on five key areas:

1. Stronger Access Controls for high-privilege users through MFA, IP whitelisting, and access audits.

2. AI Moderation Transparency via a human-in-the-loop appeal system and published review outcomes.

3. Improved DDoS Response with layered tools like CDNs, rate limiting, and WAFs.

4. User-Focused Security Education through onboarding guides, banners, and alerts.

5. Continued Use of the CISSP Framework for ongoing risk management and system design.

These strategies form a comprehensive cybersecurity roadmap to help Twitch regain trust, improve platform integrity, and proactively defend against evolving threats.

[3] Company Background & Business Challenge

Company Profile: Twitch Interactive, Inc.

Twitch is a live-streaming platform owned by Amazon, launched in 2011, and headquartered in San Francisco, California. Originally centered around video game streaming, Twitch has since expanded into a wide variety of content verticals including live music, art, "just chatting" streams, and esports broadcasting. It serves over 140 million monthly users globally, with over 2 million average concurrent viewers at any given time and more than 7 million unique streamers per month.

The Twitch platform enables real-time content broadcasting and interactive community engagement through live chat and channel-specific tools. Monetization options include subscriptions, donations, advertisements, and brand partnerships. Its infrastructure integrates live content distribution, user authentication, moderation tools, financial processing, and public APIs for developer extensions. Because of this complex and interconnected architecture, Twitch operates under high uptime requirements and zero tolerance for data compromise.

Business & Technical Challenge

Twitch's rapid growth and high visibility have made it a prime target for cyberattacks and user trust issues. Several major incidents have revealed deep flaws in both its technical systems and internal security processes:

- October 2021 Data Breach: Attackers leaked Twitch's full source code, creator earnings, and internal security tools. The breach was reportedly due to a misconfigured server with no password protection, highlighting inadequate configuration management and internal access controls.

- Frequent DDoS Attacks: Twitch streamers and infrastructure have been targeted with Distributed Denial-of-Service attacks, especially during high-visibility events. These attacks cause major disruptions, reputational damage, and financial loss.

- AI Moderation (AutoMod) Issues: Twitch's AutoMod tool, designed to reduce harassment and spam, has been criticized for bias, false positives, and a lack of transparency. Without human oversight or an appeal process, this undermines creator confidence.

- Account Hijacking and Weak IAM: Streamers and users frequently experience account takeovers due to credential stuffing and weak login protections. Internal administrative roles also lack sufficient access restrictions, increasing the risk of insider threats or accidental privilege misuse.

Strategic Importance of Solving This Challenge

As a real-time, community-driven platform, Twitch cannot afford security failures. Any compromise—whether of data, platform availability, or user trust—can immediately impact its business model, especially when monetization and brand partnerships are involved.

This capstone project addresses Twitch's urgent need for a comprehensive, risk-informed cybersecurity framework. Using CISSP principles, our goal was to deliver a set of solutions that strengthen the platform's integrity, support ethical AI use, and reinforce the trust of both streamers and viewers.

[4] Project Objectives & Scope

Project Objectives

The overarching objective of this project was to design and propose a comprehensive cybersecurity strategy for Twitch Interactive, Inc., using the CISSP (Certified Information Systems Security Professional) framework as the foundation. Our aim was to identify real-world security risks, analyze Twitch's current vulnerabilities, and apply best practices in cybersecurity governance, architecture, and risk mitigation.

Specifically, our team pursued the following goals:

1. Assess Twitch's cybersecurity posture in light of recent breaches, operational vulnerabilities, and platform-specific challenges such as real-time content delivery and user interactivity.

2. Design a role-based Identity and Access Management (IAM) model that accounts for streamers, moderators, admins, and bots—applying least privilege, multifactor authentication, and auditing.

3. Develop a CISSP-aligned Incident Response (IR) Plan, outlining how Twitch can detect, contain, eradicate, and recover from events like DDoS attacks, data breaches, and account hijacking.

4. Analyze Twitch's AutoMod system from both a technical and ethical perspective, recommending enhancements to its transparency, accountability, and reliability.

5. Deliver actionable recommendations to harden Twitch's infrastructure against cyber threats while preserving user experience and scalability.

6. Apply real-world cybersecurity frameworks to create a professional-grade solution applicable beyond Twitch's case, with relevance to other real-time, high-volume platforms.

Scope of Work

Included in Scope:

- Twitch's internal systems, including account authentication, access control policies, and backend admin operations.
- AI moderation technologies and their associated risk management concerns.
- Streamer and moderator roles and their platform privileges.
- Public API interaction (e.g., AutoMod bot access to chat functions).
- Incident response planning for large-scale disruptions or targeted attacks.
- Application of CISSP domains: IAM, Security & Risk Management, Software Development Security, and Security Operations.

Excluded from Scope:

- Twitch’s underlying cloud infrastructure that’s managed by Amazon Web Services (AWS).
- Physical data center security or on-premise hardware controls.
- Third-party vendor risk assessments (outside of public API access).
- Legal compliance issues (e.g., GDPR, CCPA) not directly tied to platform security.

This clear scope ensured that our team remained focused on Twitch’s digital security ecosystem and its core user-interactive functions, delivering depth rather than breadth. By narrowing our lens to access management, real-time threat detection, and AI moderation, we were able to create impactful, technically viable solutions tailored to Twitch’s needs.

[5] Methodology & Approach

Project Management Methodology

To guide our team workflow and ensure consistent progress across the 8-week timeline, we followed a hybrid agile-waterfall approach:

- Agile elements: Weekly meetings and iterative refinement of deliverables (especially the IAM table and incident response plan) allowed us to adjust to feedback and continuously improve.
- Waterfall elements: Our project followed a defined sequence: research → analysis → solution design → documentation → review. This ensured structured progress and aligned with milestone-based academic reporting.

We used shared Google Docs, Discord, and Canva to collaborate and track progress, with designated leads for documentation, research, visual design, workflow, and QA.

Frameworks Applied

Our primary cybersecurity framework was CISSP (Certified Information Systems Security Professional), which consists of eight core domains. The domains we focused on included:

1. Security & Risk Management:
   - Identification of ethical and business risks in AI moderation.
   - Risk assessments for role-based access and threat modeling.
2. Identity and Access Management (IAM):
   - Role mapping for streamers, moderators, admins, and bots.
   - Implementation of MFA, auto-logout, anomaly detection, and IP whitelisting.
3. Security Architecture and Engineering:
   - Secure system segmentation and credential access limits.
   - Use of layered defense for DDoS mitigation (WAF, CDN, rate-limiting).
4. Security Operations:
   - Design of a 6-step Incident Response Plan including detection, containment, and recovery.
   - Implementation of Security Information and Event Management (SIEM) systems and real-time log monitoring.
5. Software Development Security:
   - Analysis of Twitch's AI moderation tools (AutoMod) and their potential biases or vulnerabilities.
   - Recommendations for human-in-the-loop processes and transparency enhancements.

These frameworks ensured that every recommendation was rooted in industry best practices and structured thinking.

Tools and Techniques Used

To support our analysis and deliverables, we applied the following tools and techniques:

- Risk Assessment Matrix: Used to rank Twitch’s most pressing cybersecurity threats by likelihood and impact.
- IAM Role Modeling Table: Defined privilege boundaries and control mechanisms for each Twitch platform role.
- Incident Response Flow: Mapped response actions to minimize downtime and data loss.
- Security Architecture Diagram: Visualized Twitch’s system layers and access control points.
- Benchmarking: Compared Twitch’s cybersecurity practices against competitors like YouTube Live and Facebook Gaming to identify industry gaps.
- Stakeholder Mapping: Outlined executive and technical roles inside Twitch responsible for security policy execution.

This structured approach enabled our team to apply theory to practice, turning high-level CISSP domains into tailored, actionable solutions for Twitch’s complex, high-stakes environment.

[6] Findings & Analysis

Our team conducted a focused security assessment of Twitch’s platform using the CISSP framework and identified several key vulnerabilities. These findings were grouped into four major problem areas: internal access control gaps, lack of AI transparency, poor incident response readiness, and insufficient resilience to Distributed Denial-of-Service (DDoS) attacks.

Key Findings

Problem Area	Description	Impact

1. Data Breach & IAM Failures	Twitch's 2021 breach revealed leaked source code, earnings data, and internal tools. IAM systems lacked role-specific restrictions and login protections.	High reputational damage, legal risk, and loss of developer/partner trust.
2. Inadequate AI Moderation	AutoMod's opaque decision-making has led to bias, false positives, and streamer dissatisfaction. There's no appeal process or public accountability.	Erodes creator trust, damages user experience, and exposes Twitch to content moderation backlash.
3. DDoS Vulnerability	Twitch lacks layered mitigation for volumetric attacks. DDoS events have disrupted livestreams, especially during high-profile events.	Interruptions reduce ad revenue and undermine service reliability.
4. Weak Incident Response	Twitch lacks a formal Incident Response Playbook. Current processes are reactive, lacking real-time detection, playbook drills, or SIEM integration.	Increases downtime, response delays, and potential data loss in breach scenarios.

IAM Model Weaknesses

During our IAM analysis, we found that Twitch's current access control lacked key security features:

- Admins had unrestricted backend access without IP or device restrictions.
- Moderators had broad chat controls but lacked routine privilege reviews or action logging.
- AutoMod, Twitch's AI bot, had API access but no role isolation or transparency mechanisms.
- Streamers lacked advanced login detection systems and were frequent targets of credential-based attacks.

Our improved IAM model introduced:

- 2FA enforcement and auto-logout features.
- Action logging and 30-day access reviews for moderators.
- IP whitelisting, time-based access expiration, and approval workflows for admins.
- Rate-limiting and restricted task scopes for AI bots.

Incident Response Readiness

We assessed Twitch's incident response through the lens of CISSP's six-step IR lifecycle:

IR Step	Gaps Identified	Solutions Proposed
Preparation	No formal IRT training, no response playbooks, limited detection tooling.	Create IR playbook, configure SIEM, run breach simulations.
Identification	No system for real-time anomaly detection or login pattern tracking.	Integrate log monitoring and user behavior analytics.
Containment	Ad hoc account lockouts; no traffic rerouting plans.	Use Web Application Firewalls and user isolation protocols.
Eradication	Limited CVE patching or API token revocation processes.	Enforce post-breach credential revocation and token rotation.
Recovery	No staged rollout plan after breach.	Define rollback schedule, monitor logs, require password resets.
Lessons Learned	No evidence of documented post-mortems or continuous feedback loop.	Schedule post-incident reviews and update policies and detection rules.

AI Moderation (AutoMod) Analysis

AutoMod, while effective at automating moderation, suffers from three core issues:

- Lack of Transparency: There's no way for users to know why content is flagged.
- No Human Review: Decisions are final, regardless of context or community standards.
- Hard-coded Bias: Algorithms are static, leading to uneven enforcement across demographics and languages.

Recommendations include a human-in-the-loop moderation system, a feedback mechanism for flagged users, and transparency reports to publicly track AI moderation activity.

[7] Recommendations & Mitigation Plan

Based on our CISSP-driven analysis, we developed five key recommendations tailored to Twitch's most pressing cybersecurity challenges. Each recommendation includes a corresponding mitigation strategy to reduce business risk, improve operational integrity, and restore user trust.

1. Strengthen Access Controls for High-Privilege Roles

Recommendation:
Implement stricter access policies for admin and developer accounts using Multi-Factor Authentication (MFA), IP whitelisting, device binding, and role-specific access expiration.

Mitigation Strategy:

- Bind high-level accounts to verified corporate devices.
- Require login from pre-approved IP addresses only.
- Configure time-limited access credentials for elevated tasks.
- Conduct monthly access reviews and privilege audits.

Outcome:
Reduces insider threat risk, mitigates privilege escalation attacks, and ensures access aligns with business necessity.

2. Enhance AI Moderation Transparency and Accountability

Recommendation:
Redesign the AutoMod moderation pipeline to include human-in-the-loop review capabilities and a public-facing appeal system.

Mitigation Strategy:

- Create a content appeal form integrated into Twitch's moderation workflow.
- Establish thresholds for AutoMod actions that require human approval.

Outcome:
Restores creator trust, addresses ethical concerns around algorithmic bias, and introduces a feedback loop to improve AutoMod performance.

3. Improve DDoS Detection and Response Capabilities

Recommendation:
Deploy layered defense tools to detect and absorb volumetric attacks, especially during major live events.

Mitigation Strategy:

- Integrate Web Application Firewall (WAF) with Twitch's CDN infrastructure.
- Use behavioral rate limiting to throttle malicious traffic patterns.
- Implement cloud-based DDoS mitigation services that auto-scale.

Outcome:
Ensures service availability, protects user experience, and strengthens Twitch's operational resilience during peak traffic periods.

4. Launch Platform-Wide Security Education Campaign

Recommendation:
Educate creators and users about account protection, phishing awareness, and Twitch's security features through targeted campaigns.

Mitigation Strategy:

- Embed security tips in user onboarding and settings pages.
- Use banners, short videos, and in-app alerts to share advice.

- Partner with top creators to promote best practices.

Outcome:
Empowers users to protect themselves, reduces attack surface, and builds a culture of shared cybersecurity responsibility.

5. Institutionalize CISSP as Twitch's Security Planning Framework

Recommendation:
Use CISSP domains to guide future security investments, organizational training, and technology evaluations.

Mitigation Strategy:

- Align new policies and infrastructure with CISSP pillars: IAM, risk management, operations, and software security.
- Develop red team/blue team simulations to train internal staff.
- Apply CISSP audit criteria to evaluate third-party security vendors.

Outcome:
Creates a repeatable, industry-aligned process for continuous cybersecurity improvement across all departments.

These recommendations form an integrated cybersecurity roadmap, designed not only to remediate current vulnerabilities, but to evolve with Twitch's future scaling and technological demands.

[8] Project Deliverables Summary

The following table outlines the major deliverables produced throughout the project lifecycle. Each deliverable was developed using CISSP principles and targeted one or more of Twitch's identified cybersecurity vulnerabilities.

Deliverable	Description	Framework Domain(s)

Security Architecture Diagram	A high-level system diagram identifying Twitch's critical access points, segmented components, and security zones.	Security Architecture & Engineering
Enhanced IAM Role Model Table	A detailed table outlining platform roles (Streamer, Moderator, Admin, AutoMod), their access levels, authentication methods, and controls.	Identity & Access Management (IAM)
CISSP-Aligned Incident Response Plan	A six-step IR playbook including Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned tailored for Twitch.	Security Operations
AI Moderation Risk Assessment	An evaluation of AutoMod's weaknesses related to transparency, bias, and trust, with proposals for ethical oversight and appeal mechanisms.	Security & Risk Management, Software Security
Final Recommendations Summary	A five-part strategic roadmap covering IAM controls, AI transparency, DDoS protection, user education, and CISSP institutionalization.	Multi-domain (Risk, IAM, Ops, Dev Security)
Executive Presentation (Slides)	A visually engaging summary of all findings, deliverables, and recommendations, presented to stakeholders.	Communication & Stakeholder Engagement
Final Report Document	This comprehensive written report detailing all aspects of the project: objectives, findings, analysis, and recommendations.	All CISSP Domains (Capstone Integration)

Each deliverable was collaboratively reviewed and refined to ensure consistency, clarity, and alignment with real-world cybersecurity standards. Together, they form a comprehensive security framework that Twitch could realistically adopt and adapt for long-term resilience.

[9] Reflection & Learning

Group Reflection

Working on the Twitch cybersecurity framework project was an intensive and eye-opening experience for our entire team. As students, we were already familiar with basic security concepts, but this project challenged us to apply those principles in a real-world context with high stakes, technical complexity, and visible consequences.

One of the most important things we learned is that cybersecurity is not just a technical challenge—it's also a problem of governance, ethics, and communication. Whether we were designing access models, drafting an incident response plan, or analyzing AI moderation, we had to consider not only how systems worked, but how people would interact with them. This helped us gain a deeper understanding of security as a business enabler, not just a cost center.

We also discovered how essential frameworks like CISSP are in bringing structure and clarity to complex problems. The eight domains helped us break down Twitch's challenges into manageable categories and made it easier to assign responsibilities within the team. Every deliverable we produced tied back to a specific domain, which ensured that our work stayed grounded in industry standards.

Time management, iterative development, and peer feedback were also major learning experiences. At one point, we received feedback that our IAM model was "too barebones," and instead of getting discouraged, we took it as an opportunity to build something more in-depth. The final product was stronger as a result of that revision process.

Individual Learning Highlights

- Rochan Aminzadeh (QA Reviewer):
  "I learned the importance of quality control and cross-functional review. By checking our work for consistency and clarity, I realized how critical communication is in cybersecurity—especially when policies affect technical and non-technical users alike."

- Abdullah Bhatti (Documentation Lead):
  "This project sharpened my ability to translate technical ideas into professional documentation. I also gained confidence in risk analysis and policy writing, which are essential for anyone going into cybersecurity consulting or compliance."

- Vito Mkrtychyan (Workflow Coordinator):
  "Coordinating deliverables taught me the value of structure and accountability. Even a

strong technical solution can fail if it’s delivered late or isn’t communicated clearly. The hybrid agile-waterfall method we used worked really well.”

- Dennis Nazarchuk (Research Lead):
  “I enjoyed digging into Twitch’s security incidents and industry benchmarks. Doing a threat model for a real company made me realize how much is at stake when data and trust are compromised.”

- Aqdas Tanweer (Visual Design Lead):
  “I learned how to turn complex security models into visuals that are easy to understand. Good design plays a huge role in making technical solutions accessible to decision-makers and users.”

This project not only helped us grow as cybersecurity students, but also as collaborators, thinkers, and future professionals in the field of IT and information systems.

Link to presentation:
https://www.canva.com/design/DAGoTlIIeSs/cHNy_Mc8ae5Fy4iJJ64Q8Q/edit

[10] References

1. **(ISC)² CISSP Official Study Guide** – Eighth Edition
   Authors: Mike Chapple & James Michael Stewart
   Used to define and apply the eight CISSP domains to Twitch’s real-world cybersecurity challenges.

2. **Twitch Data Breach Report (2021)**
   Source: The Verge – “Twitch confirms massive data breach after its source code and secrets leak out”
   URL: https://www.theverge.com
   Referenced to understand the scope and impact of Twitch’s security vulnerabilities.

3. **OWASP Secure Software Development Guidelines**
   Source: Open Web Application Security Project (OWASP)
   Used to evaluate Twitch’s AutoMod system and software development practices.

4. **Cloudflare Learning Center – What is a DDoS Attack?**
   URL: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack
   Used to guide DDoS mitigation strategies through layered defense mechanisms.

5. **Twitch Developer Documentation – API & Bot Integration**
   URL: https://dev.twitch.tv/docs
   Used to evaluate the AutoMod system and limitations on bot access through public APIs.

6. **Harvard Business Review – Cybersecurity is a Strategic Issue**
   Author: Thomas Parenty & Jack Domet
   Emphasized the strategic business impact of security failures and leadership responsibilities.

7. **YouTube Live & Facebook Gaming Security Practices**
   (Benchmarked via public-facing articles and platform documentation)
   Used for comparison against Twitch's IAM structure, transparency features, and incident response maturity.

8. **Slack Security Whitepaper (2023)**
   Reference for role-based IAM, device whitelisting, and anomaly detection practices in modern platforms.

9. **MIT Technology Review – "The Problem with AI Moderation"**
   Referenced to analyze AutoMod's ethical limitations and the need for human-in-the-loop processes.