💼 Executive Summary

💼 Executive Summary

Our assessment identifies three high-impact threat actors targeting the new gaming add-on: Organized Cybercriminals, Nation-State Groups, and Insider Threats. Cybercriminals seek financial gain through account takeover, payment fraud, and stolen digital assets. Nation-state actors are motivated by political leverage and disruption, especially because the platform has U.S. government users, raising the risk of targeted intrusion campaigns. Insider threats—whether negligent or malicious—pose operational risks, including data mishandling, credential abuse, or unauthorized system access.

These actors use well-known attack paths such as phishing, credential theft, privilege escalation, supply-chain compromise, and abuse of cloud infrastructure. Their techniques can disrupt revenue, erode user trust, and expose the company to liability. Together, these threat actors represent the most realistic combination of likelihood and impact, targeting the company's intellectual property, user data, and reputation.

For executives, this model clarifies which threats could impact brand reputation and launch success. For IT, it maps realistic adversary behaviors to known detection gaps. For legal, it highlights risks involving regulated users and data that could trigger compliance or reporting obligations.

Our solution roadmap prioritizes defenses that give the startup immediate visibility, measurable risk reduction, and compliance support. The top honeypot recommendation deploys a lightweight deception system to attract attackers early and reveal their methods without impacting production systems—providing IT with actionable alerts and Legal with clear evidence trails. The top data-source priority is DS0009, which offers broad visibility into lateral movement, credential misuse, and exfiltration attempts. This helps IT teams detect threats earlier while also creating auditable records that support legal and regulatory requirements. The top mitigation recommendation is a cloud-native Web Application Firewall (WAF), which blocks common attack paths such as injection, credential stuffing, and API abuse. This reduces exploitation risk, protects sensitive player data, and supports executives by ensuring a secure and stable public launch.

Together, these solutions build a practical, scalable defense aligned with the company's startup environment and public-facing risks.These solutions balance operational feasibility, startup budgets, and stakeholder needs.

Executives gain confidence in launch readiness. IT gains practical tools that reduce alert fatigue and strengthen detection. Legal gains improved evidence retention, due-diligence posture, and regulatory defensibility.

Threat Model

Threat Model for Xibalba Interactive

🥷 Threat Actors

🥷 Threat Actors

1. THREAT ACTORP: Cybercriminals

Cybercriminals are the most likely to attack a gaming platform because; Gaming sites involve payment processing, a direct financial target.New public web features + APIs make attractive targets for automation-based attacks.Chat systems and gamer accounts are valuable for fraud, phishing, scams, and account resale. Startups often have immature security programs, making them perfect opportunities. Cybercriminals attack gaming companies every day, making them your #1 threat.Cybercriminals are primarily motivated by financial gain

2. THREAT ACTOR: Insider Threats

Your environment has several insider-sensitive areas:Developers with access to IP and source code.Cloud storage buckets containing logs and PII. Administrators with access to chat logs, which include U.S. government employees. Payment-processing and database servers. A small startup means fewer checks and balances, making insider misuse more likely.In gaming startups, insiders are consistently a top threat due to privileged access and lack of monitoring.Insiders may be motivated by: Financial need, Disgruntlement or job dissatisfaction,Opportunity through poor oversight, Curiosity, Coercion or bribery by external actors They often target data that is easy to access internally: logs, player data, IP, chat histories.

3. THREAT ACTOR: Advanced Persistent Threats (APTs) / Nation-State Actors

Your platform hosts U.S. government employees who use the chat feature, which dramatically elevates your risk profile. APTs are relevant because: They target government personnel, even off-duty. In-game chats and messaging have been used for covert communication monitoring and social engineering. Your system could be used as a foothold to perform reconnaissance on U.S. government staff. APTs often attack gaming platforms to collect metadata, behavioral indicators, and social connections. Even if the company is “just a gaming startup,” the presence of U.S. government users raises the threat level significantly.APTs/Nation-State actors are motivated by: Intelligence gathering,Identifying or tracking government personnel, Monitoring chat traffic for sensitive communications, Collecting metadata on relationships, habits, or patterns, Compromising a platform to move toward higher-value government targets, Sabotage or destabilization.

⚔️ Attack Surface

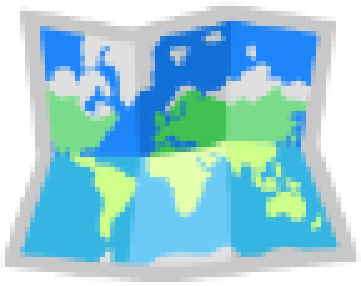
⚔️ Attack Surface

Attack Surface	Asset(s)	ATT&CK TTPs	Likelihood	Impact
admin or support misuse	Payment Card Information (PCI)	T1547 — Boot or Logon Autostart Execution, T1059 — Command and Scripting Interpreter, T1005 — Data from Local System, T1204 — User Execution, T1040 -Network Sniffing, T1087 — Account Discovery, T1098 — Account Manipulation, T1505 — Server Software Component	4 (Like…	4 (Major)
API and game code	Intellectural Property (IP)	• TTP ID (TTP Name)	4 (Like…	5 (Cata…
Chat applications	In-game private chat system	• TTP ID (TTP Name)	3 (Pos…	3 (Mod…
cloud storage	Intellectural Property (IP)	• TTP ID (TTP Name)	4 (Like…	5 (Cata…
credentials database	Personally Identifiable Information(PII)	• TTP ID (TTP Name)	3 (Pos…	4 (Major)
credit card info	Payment Card Information (PCI)	• TTP ID (TTP Name)	3 (Pos…	4 (Major)
Data logs	In-game private chat system	• TTP ID (TTP Name)	3 (Pos…	5 (Cata…
database	Personally Identifiable Information(PII)	• TTP ID (TTP Name)	2 (Unli…	5 (Cata…
database server	Personally Identifiable Information(PII)	• TTP ID (TTP Name)	2 (Unli…	5 (Cata…
Developers	Intellectural Property (IP)	T1547 — Boot or Logon Autostart Execution,	4 (Like…	5 (Cata…

Attack Surface	Asset(s)	ATT&CK TTPs	Likelihood	Impact
		T1059 — Command and Scripting Interpreter, T1005 — Data from Local System, T1204 — User Execution, T1040 -Network Sniffing, T1087 — Account Discovery, T1098 — Account Manipulation, T1505 — Server Software Component		
Developers workstations	Personally Identifiable Information(PII)	T1547 — Boot or Logon Autostart Execution, T1059 — Command and Scripting Interpreter, T1005 — Data from Local System, T1204 — User Execution, T1040 -Network Sniffing, T1087 — Account Discovery, T1098 — Account Manipulation, T1505 — Server Software Component	3 (Pos…	4 (Major)
gamers	Payment Card Information (PCI)	T1190 — Exploit Public-Facing Application, T1078 — Valid Accounts	5 (Alm…	3 (Mod…
Gamers/Users	Personally Identifiable Information(PII)	T1190 — Exploit Public-Facing Application, T1547 — Boot or Logon Autostart Execution, T1059 — Command and Scripting Interpreter	5 (Alm…	3 (Mod…
js,express,git	Intellectural Property (IP)	T1530 — Data from Cloud Storage Object, T1078 — Valid Accounts, T1041 — Exfiltration Over C2 Channel	3 (Pos…	4 (Major)
network traffice	Payment Card Information (PCI)	T1059 — Command and Scripting Interpreter, T1530 — Data from Cloud Storage Object, T1005 — Data from	3 (Pos…	4 (Major)

Attack Surface	Asset(s)	ATT&CK TTPs	Likelihood	Impact
		Local System		
payment proccessing server	Payment Card Information (PCI)	T1059 — Command and Scripting Interpreter, T1530 — Data from Cloud Storage Object, T1005 — Data from Local System	3 (Pos…	5 (Cata…
Production and development servers	Intellectural Property (IP)	T1190 — Exploit Public-Facing Application, T1530 — Data from Cloud Storage Object, T1041 — Exfiltration Over C2 Channel	3 (Pos…	4 (Major)
support staff/moderators	In-game private chat system	T1078 — Valid Accounts	4 (Like…	5 (Cata…
web payment server	Payment Card Information (PCI)	T1190 — Exploit Public-Facing Application, T1059 — Command and Scripting Interpreter, T1071 — Application Layer Protocol	3 (Pos…	4 (Major)
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…
		• TTP ID (TTP Name)	1 (Rare)	1 (Insig…

🗺️ Solution Roadmap



Solution Roadmap for Xibalba Interactive

🍯 Honey strategies

🍯 Honey strategy Solutions:

🍯 Honeypot Solution #1		
Solution #1 Web Bug	**Difficulty:** 1 (Easy)	**Priority:** 3 (High)
The honeypot mimics game APIs, dev endpoints, or admin panels, and silently records attacker behavior. This gives the security team early warning and high-confidence detection of malicious activity targeting the platform.		
Addresses attack vector(s):	T1595, T1110, T1190, T1059, T1071, T1041, T1087	
Protects key asset(s):	IP, PII, In game chat, PCI	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
Provides *early warning* of targeted attacks before real damage.Minimal cost, high ROI, boosts investor confidence. Helps protect brand reputation during public launch and reduces breach likelihood without slowing development.	Gives real-time, high-fidelity alerts with *near-zero false positives*. Reveals attacker techniques that inform firewall rules and API hardening. Helps the team understand which assets attackers target first. Less alert fatigue, clearer prioritization, stronger detection coverage.	Provides defensible logs showing proactive monitoring. Strengthens incident response documentation and due diligence. Reduces regulatory liability and improves audit posture.
GOALS		
Name	**Description**	**Deadline**
Set up a deceptive endpoint and monitor all access attempts with automated alerting.	Addresses early-stage attack behaviors before they hit real servers.	Fully enabled in 30 days

Collect and analyze attacker telemetry from the honeypot to improve detection rules and strengthen defensive configurations.	Capture IP addresses, payloads, HTTP headers, authentication attempts, user agents, and attack patterns. Improves threat intelligence and closes visibility gaps for a high-risk public launch.	60 days, update every quarter
ADD GOAL #3 NAME HERE		

🍯 Honeypot Solution #2		
Solution #2 NAME HERE	**Difficulty:** 1 (Easy)	**Priority:** 1 (Low)
ADD SOLUTION SUMMARY HERE		
Addresses attack vector(s):	- LIST RELEVANT ATT&CK TTPs HERE	
Protects key asset(s):	- LIST RELEVANT KEY ASSETS HERE	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
ADD EXECUTIVE ARGUMENT HERE.	ADD IT TEAM ARGUMENT HERE.	ADD LEGAL ARGUMENT HERE.
GOALS		
Name	**Description**	**Deadline**
ADD GOAL #1 NAME HERE		
ADD GOAL #2 NAME HERE		
ADD GOAL #3 NAME HERE		

🍯 Honeypot Solution #3		
Solution #3 NAME HERE	**Difficulty:** 1 (Easy)	**Priority:** 1 (Low)
ADD SOLUTION SUMMARY HERE		
Addresses attack vector(s):	- LIST RELEVANT ATT&CK TTPs HERE	

Protects key asset(s):	- LIST RELEVANT KEY ASSETS HERE	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
ADD EXECUTIVE ARGUMENT HERE.	ADD IT TEAM ARGUMENT HERE.	ADD LEGAL ARGUMENT HERE.
GOALS		
Name	**Description**	**Deadline**
ADD GOAL #1 NAME HERE		
ADD GOAL #2 NAME HERE		
ADD GOAL #3 NAME HERE		

🍯 Honeypot Solution #4		
Solution #4 NAME HERE	**Difficulty:** 1 (Easy)	**Priority:** 1 (Low)
ADD SOLUTION SUMMARY HERE		
Addresses attack vector(s):	- LIST RELEVANT ATT&CK TTPs HERE	
Protects key asset(s):	- LIST RELEVANT KEY ASSETS HERE	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
ADD EXECUTIVE ARGUMENT HERE.	ADD IT TEAM ARGUMENT HERE.	ADD LEGAL ARGUMENT HERE.
GOALS		
Name	**Description**	**Deadline**
ADD GOAL #1 NAME HERE		
ADD GOAL #2 NAME HERE		
ADD GOAL #3 NAME HERE		

🍯 Honeypot Solution #5		
Solution #5 NAME HERE	**Difficulty:** 1 (Easy)	**Priority:** 1 (Low)
ADD SOLUTION SUMMARY HERE		
Addresses attack vector(s):	- LIST RELEVANT ATT&CK TTPs HERE	
Protects key asset(s):	- LIST RELEVANT KEY ASSETS HERE	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
ADD EXECUTIVE ARGUMENT HERE.	ADD IT TEAM ARGUMENT HERE.	ADD LEGAL ARGUMENT HERE.
GOALS		
Name	**Description**	**Deadline**
ADD GOAL #1 NAME HERE		
ADD GOAL #2 NAME HERE		
ADD GOAL #3 NAME HERE		

📊 Data sources

📊 Data Sources:

📊 Data Source Solution #1

Solution #1 DS0009	**Difficulty:** 1 (Easy)	**Priority:** 3 (High)
Monitor for API calls that may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.		
Addresses attack vector(s):	- T1547 — Boot or Logon Autostart Execution, T1059 — Command and Scripting Interpreter, T1005 — Data from Local System, T1204 — User Execution, T1040 -Network Sniffing, T1087 — Account Discovery, T1098 — Account Manipulation, T1505 — Server Software Component	

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
You get early detection of attackers, preventing PR disasters, lost users, and downtime. This protects the brand and revenue.	You gain visibility into how systems communicate, making it much easier to spot intrusions and fix misconfigurations.	Reduced risk of unauthorized access to PII or payment data lowers liability and strengthens your incident-response defensibility.

GOALS		
Name	**Description**	**Deadline**
Implement network flow monitoring to detect abnormal outbound traffic indicating data exfiltration.	Collect NetFlow/VPC Flow logs for all cloud and production segments.	Fully enabled in 30 days
Detect adversary-in-the-middle attacks or internal sniffing attempts.	Monitor for ARP spoofing, unexpected DNS traffic, and unusual internal scanning.	Detection rules created and validated within 45 days.

📊 Data Source Solution #2

Solution #2 DS0012	**Difficulty:** 2 (Medium)	**Priority:** 3 (High)
Monitor for any attempts to enable scripts running on a system that would be considered suspicious.		
Addresses attack vector(s):	- T1059 — Command and Scripting Interpreter, T1005 — Data from Local System	

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
Prevents catastrophic reputation damage caused by tampered game updates or compromised payment pages.	.Gives instant alerts when someone changes production code, cutting incident detection time significantly.	Helps prove compliance with PCI and security frameworks in audits or lawsuits.

GOALS		
Name	**Description**	**Deadline**
Monitor for suspicious certificate creation, modification, or trust-store changes.	Alert when certificates are replaced or added without approval.	Implemented within 60 days.
Track certificate misuse in internal apps such as API servers or payment gateways.	Log failed certificate validation attempts or expired certificate use.	Insights produced within 45 days.
ADD GOAL #3 NAME HERE		

📊 Data Source Solution #3

Solution #3 DS0017	**Difficulty:** 2 (Medium)	**Priority:** 3 (High)
Monitor executed commands and arguments that may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems.		
Addresses attack vector(s):	- T1547 — Boot or Logon Autostart Execution, T1041 — Exfiltration Over C2 Channel, T1059 — Command and Scripting Interpreter, T1005 — Data	

	from Local System, T1204 — User Execution, T1040 -Network Sniffing, T1087 — Account Discovery, T1098 — Account Manipulation, T1505 — Server Software Component, T1110-Brute Force

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
Keeps the site available for players, protects brand trust, and reduces downtime.	Provides real-time insight into active attacks and reduces the burden of manual log review.	WAF logs help demonstrate due diligence, which is critical in the event of regulatory investigations.

GOALS		
Name	**Description**	**Deadline**
Monitor DNS queries for suspicious or newly registered domains used for phishing or C2.	Correlate traffic with threat-intel feeds and new domain age lookups.	Enabled within 30 days.
Detect internal domain hijacking or subdomain takeover attempts.	Alert on unauthorized DNS record changes (A, CNAME, MX).	Fully deployed within 60 days.
ADD GOAL #3 NAME HERE		

📊 Data Source Solution #4

Solution #4 DS0022	**Difficulty:** 2 (Medium)	**Priority:** 3 (High)
Use verification of distributed binaries through hash checking or other integrity checking mechanisms		
Addresses attack vector(s):	- T1195 — Supply Chain Compromise, T1566.002 — Phishing, T1566 — Phishing, T1195.001 — Compromise Software Dependencies and Development Tools, T1195 Supply Chain Compromise, T1547 — Boot or Logon Autostart Execution, T1041 — Exfiltration Over C2 Channel, T1005 — Data from Local System, T1204 — User Execution, T1087 — Account Discovery, T1098 — Account Manipulation, T1505 — Server Software Component	

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
Protects users (including government employees) and reduces liability from chat-based abuse or account takeovers.	Gives essential visibility to debug incidents, trace attacks, and identify flawed behaviors.	Application logs provide evidentiary trails necessary for investigations and compliance reporting.

GOALS

Name	Description	Deadline
Log and alert on suspicious file creation, such as new executables or scripts in sensitive directories.	Monitor for unexpected file drops in servers, CI/CD, and payment systems	Implement in 30 days.
Track sensitive data file creation, such as new credit-card dumps or chat log copies.	Alert when files containing PII/card data appear outside approved paths.	Fully operational in 45 days.
ADD GOAL #3 NAME HERE		

📊 Data Source Solution #5

Solution #5 DS0029	Difficulty: 1 (Easy)	Priority: 1 (Low)
Use deep packet inspection to look for artifacts of common exploit traffic, such as SQL injection strings or known payloads.		
Addresses attack vector(s):	- T1190 — Exploit Public-Facing Application, T1566 — Phishing, T1566.002 — Phishing, T1041 — Exfiltration Over C2 Channel, T1204 — User Execution, T1071 — Application Layer Protocol, T1505 — Server Software Component	

STAKEHOLDERS

Executives	IT Team	Legal
Prevents the worst-case scenario: loss of sensitive player/PII data and a massive public breach.	Provides forensic detail, enabling fast containment and post-incident analysis.	Database logs are often required for compliance, audit trails, and breach reporting laws.

GOALS

Name	Description	Deadline
Detect any attempt to access or dump OS credentials from memory, SAM, LSASS, or cloud token caches.	Monitor LSASS access, token extraction attempts, and abnormal privilege use.	Implemented in 35 days.
Harden systems to prevent credential dumping and reduce credential exposure.	Enforce Credential Guard equivalents, disable WDigest, and implement least-privilege admin separation.	Completed within 90 days.
ADD GOAL #3 NAME HERE		

🔮 Mitigations

🔮 Preventive Mitigations:

🔮 Preventive Solution #1

Solution #1 M1018	**Difficulty:** 1 (Easy)	**Priority:** 3 (High)
Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts. Regularly check component software on critical services that adversaries may target for persistence to verify the integrity of the systems and identify if unexpected changes have been made.		
Addresses attack vector(s):	- T1110-Brute Force, T1098 — Account Manipulation, T1505 — Server Software Component, T1087 — Account Discovery, T1040 -Network Sniffing, T1530 — Data from Cloud Storage Object, T1195 — Supply Chain Compromise, T1078 — Valid Accounts	

STAKEHOLDERS		
Executives	**IT Team**	**Legal**
You get early detection of attackers, preventing PR disasters, lost users, and downtime. This protects the brand and revenue.	You gain visibility into how systems communicate, making it much easier to spot intrusions and fix misconfigurations.	Reduced risk of unauthorized access to PII or payment data lowers liability and strengthens your incident-response defensibility.

GOALS		
Name	**Description**	**Deadline**
Deploy RBAC and MFA across all development, admin, and cloud accounts to ensure least-privilege access	Define and enforce roles for developers, admins, support staff, and contractors. Enable MFA for all privileged and cloud accounts Directly reduces the likelihood of account takeover—one of the highest risks for this product.	Complete within 45–60 days
Implement automated user provisioning and quarterly access reviews to limit dormant or excessive accounts	Integrate HR processes with IAM; disable accounts automatically on termination; run quarterly access audits. Addresses insider threats, regulatory exposure, and operational mistakes.	Implementation within 90 days, quarterly reviews ongoing thereafter.
ADD GOAL #3 NAME HERE		

🔮 Preventive Solution #2

Solution #2 M1026	**Difficulty:** 1 (Easy)	**Priority:** 1 (Low)
Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.		
Addresses attack vector(s):	- T1098 — Account Manipulation, T1505 — Server Software Component, T1059 — Command and Scripting Interpreter, T1078 — Valid Accounts	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
You get early detection of attackers, preventing PR disasters, lost users, and downtime. This protects the brand and revenue.	You gain visibility into how systems communicate, making it much easier to spot intrusions and fix misconfigurations.	Reduced risk of unauthorized access to PII or payment data lowers liability and strengthens your incident-response defensibility.
GOALS		
Name	**Description**	**Deadline**
Deploy a PAM system to control, audit, and time-limit all administrator and developer elevated actions.	Implement a PAM tool to enforce JIT access, mandatory approvals, and session recording for all production-admin actions. Directly mitigates risks from cybercriminals and insider threats—both of which rely heavily on compromised or misused privileged accounts.	60-75 days fully
Eliminate persistent admin accounts by enforcing least-privilege baselines and implementing separate user/admin identities for all technical staff.	Remove standing admin rights, require developers and IT staff to maintain separate daily-use and admin accounts, and enforce automatic privilege expiration. Reduces attack surface, prevents privilege escalation, and maintains compliance readiness for payment systems and government-affiliated users.	45-60 days
ADD GOAL #3 NAME HERE		

🔮 Preventive Solution #3

Solution #3 M1032	**Difficulty:** 1 (Easy)	**Priority:** 3 (High)
Use multi-factor authentication. Where possible, also enable multi-factor authentication on externally facing services.		

Addresses attack vector(s):	- T1110-Brute Force, T1098 — Account Manipulation, T1040 -Network Sniffing, T1530 — Data from Cloud Storage Object, T1078 — Valid Accounts	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
MFA significantly reduces the chance of a breach that could damage the brand, delay product launch, or expose high-profile users (including U.S. government players). It is one of the fastest and most cost-effective risk reducers. This gives stronger investor confidence, lowers financial risk,and gives faster compliance readiness	Reduces the number of urgent security incidents caused by stolen credentials. MFA protects access to cloud consoles, code repos, and deployment systems. These are core areas targeted by attackers. They will value this because there is less time responding to identity compromise incidents, stronger protection for production environments, and this gives clear audit trails to support troubleshooting	MFA is a common requirement in regulatory frameworks.This reduces the likelihood of a breach involving government-affiliated users, which would trigger major reporting obligations. This demonstrates security controls reducing liability, ensures alignment with future contract requirements, and helps meet disclosure and retention obligations with clean authentication logs
GOALS		
Name	**Description**	**Deadline**
Require MFA for all privileged accounts and administrative tools across the development and production environments.	Directly prevents 90% of credential-based attacks (credential stuffing, phishing, brute force).	30 days
Implement MFA for internal developer and employee accounts with automated enforcement and user onboarding.	Roll out MFA to all internal users. Reduces risk of insider misuse, phishing, and lateral movement—addressing major risks for the gaming add-on platform.	45 days
ADD GOAL #3 NAME HERE		