💼 Executive Summary

💼 Executive Summary

After performing a threat model for Xibalba we were able to identify the most likely threat actors, attack surfaces & key solutions to mitigate potential risks posed.

The primary identified threat actors are: Cybercriminals, Insider Threats & Nation State Actors.

- Cyber criminals might target the company to steal personal/financial/PII data & sell it on the Dark Web. Examples might include Phishing attacks & other malicious attacks.
- Insider threats include financial incentives from competitors, the selling of sensitive information for profit or revenge against the organization.
- Nation State Actors use propaganda campaigns (”psyops”) to influence public opinion. It may also lead to gaining economic or technological advances.

Attack Surfaces include but are not limited to, developers, the game & API, end users/developers, weak passwords, GitFolders, the developers laptop, the cloud servers & private servers, & the computer/web server.

Key solutions to mitigate these risks include the use of various HoneyPots such as HoneyMail, HoneyTokens & HoneyFiles. Data Sources should include Application Log Management (DS0015). The mitigations recommended are User Training (M1017), User Account Management (M1018), & Vulnerability Scanning (M1016).

After implementing the suggestions given in the threat model, Xibalba will have a better security posture. Our recommendations will help Xibalba stay in compliance & save money.

♨️ Threat Model

Threat Model for Xibalba Interactive

🥷 Threat Actors

🥷 Threat Actors

1. Cyber-Criminals
Cyber criminals might target the company to steal personal/financial/PII data & sell it on the Dark Web. Examples might include Phishing attacks & other malicious attacks.

- **SCENARIO:** The attacker used a payload to run a command allowing access to remote viewing and capture keylogged information. This is a form of data exfiltration. A script could be employed to relay information back to the attacker undetected.

2. Insider Threats
Insider Threats include financial incentives from competitors, the selling of sensitive information for profit or revenge against the organization.

- **SCENARIO:** Company downsizing could lead to a disgruntled employee who then decides to wreak havoc on company systems before leaving or decides to sell company secrets on the black market.

3. Nation State Actors
Propaganda campaigns (”psyops”) could be used to influence public opinion. It may also lead to gaining economic or technological advances.

- **SCENARIO:** Nation State Actors may use in-game-chats to relay secret messages covertly. They may wish to sway a political election or they might want to know if this game code can in any way benefit their own endeavors.

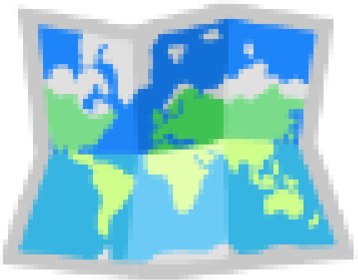
⚔️ Attack Surface

⚔️ Attack Surface

Attack Surface	Asset(s)	ATT&CK TTPs	Likelihood	Impact
Gamers & Users	PII	**T1566: Phishing**	5 (Alm…	5 (Cata…
Developers	IP	**T1078: Valid Accounts**	4 (Like…	4 (Major)
Game & API	IP	**T1190: Exploit Public Facing**	4 (Like…	4 (Major)
Gamers or Developers	IP PII	**T1586: Compromise Accounts**	4 (Like…	4 (Major)
Weak Passwords	IP PII PCI	**T1110: Brute Force**	2 (Unli…	5 (Cata…
GitFolder	IP	**T1567: Exfiltration Over Web Service**	1 (Rare)	1 (Insig…
Developer Laptop	IP PII PCI	**T1119: Automated Collection**	3 (Pos…	5 (Cata…
Cloud Servers & Private Servers	IP PII PCI	**T1505: Server Software Component: SQL Stored Procedures**	4 (Like…	4 (Major)
Gamers	IP	**T1036: Masquerading**	4 (Like…	5 (Cata…
Gamers & Developers	IP PII PCI	**T1528: Steal Application Access Token**	3 (Pos…	5 (Cata…
Gamers & Developers	IP PII PCI	**T1189: Drive by Compromise**	3 (Pos…	5 (Cata…
Computer/Web Server	IP PII PCI	**T1133: External Remote Services**	1 (Rare)	1 (Insig…

Attack Surface	Asset(s)	ATT&CK TTPs	Likelihood	Impact
		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…
		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 HoneyToken	**Difficulty:** 1 (Easy)	**Priority:** 2 (Medium)
Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls.		
Addresses attack vector(s):	T1528: Steal Application Access Token	
Protects key asset(s):	IP PII PCI	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
It is a low cost, low resource solution that provides protective/detective capabilities.	It is a low cost, low resource solution that provides protective/detective capabilities.	Early detection will strengthen the company's security position.
GOALS		
Name	**Description**	**Deadline**
GOAL #1 Implement Honeypot	Deploy honeypots to increase visibility.	They should be implemented within 3 months.
GOAL #2 User account management	Strengthen account management practices.	2 months

🍯 Honeypot Solution #2

Solution #2 HoneyFile	**Difficulty:** 1 (Easy)	**Priority:** 2 (Medium)

Create a fake code repository to entice attackers to the HoneyFile as an early alarm system.		
Addresses attack vector(s):	T1567: Exfiltration Over Web Service, T1020: Automated Exfiltration	
Protects key asset(s):	IP PII PCI	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
It is a low cost, low resource solution that provides protective/detective capabilities.	It is a low cost, low resource solution that provides protective/detective capabilities.	Early detection will strengthen the company's security position.
GOALS		
Name	**Description**	**Deadline**
GOAL #1 Implement Honeypot	Deploy honeypots to increase visibility.	They should be implemented within 3 months.
GOAL #2 User account management	Strengthen account management practices.	2 months

🍯 Honeypot Solution #3

Solution #3 HoneyMail	**Difficulty:** 1 (Easy) ▾	**Priority:** 2 (Medium) ▾
Setting up fake email accounts & if these accounts start to receive mail, something is obviously wrong. Uses a set of email addresses to identify phishing campaigns.		
Addresses attack vector(s):	T1566: Phishing, T1078: Valid Accounts	
Protects key asset(s):	IP PII PCI	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
It is a low cost, low resource solution that provides	It is a low cost, low resource solution that provides	Early detection will strengthen the company's security position.

protective/detective capabilities.	protective/detective capabilities.	
GOALS		
Name	**Description**	**Deadline**
GOAL #1 Implement Honeypot	Deploy honeypots to increase visibility.	They should be implemented within 3 months.
GOAL #2 User account management	Strengthen account management practices.	2 months

🍯 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 DS0015 - Application Log Management	**Difficulty:** 1 (Easy)	**Priority:** 1 (Low)

Monitor authentication logs for system and application login failures of Valid Accounts. If authentication failures are high, then there may be a brute force attempt to gain access to a system using legitimate credentials.

Monitor for third-party application logging, messaging, and/or other artifacts that may send phishing messages to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed. URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.

Monitor call logs from corporate devices to identify patterns of potential voice phishing, such as calls to/from known malicious phone numbers. Correlate these records with system events.

When authentication is not required to access an exposed remote service, monitor for follow-on activities such as anomalous external use of the exposed API or application.Configuration management databases (CMDB) and other asset management systems may help with the detection of computer systems or network devices that should not exist on a network.

Configuration management databases (CMDB) and other asset management systems may help with the detection of computer systems or network devices that should not exist on a network.

Monitor for third-party application logging, messaging, and/or other artifacts that may abuse legitimate extensible development features of servers to establish persistent access to systems. Consider monitoring application logs for abnormal behavior that may indicate suspicious installation of application software components. Log authentication attempts to the server and any unusual traffic patterns to or from the server and internal network.

Monitor email gateways usually do not scan internal email, but an organization can leverage the journaling-based solution which sends a copy of emails to a security service for offline analysis or incorporate service-integrated solutions using on-premise or API-based integrations to help detect internal spearphishing attacks.

Detecting software exploitation may be difficult depending on the tools available. Software exploits may not always succeed or may cause the exploited process to become unstable or crash. Web Application Firewalls may detect improper inputs attempting exploitation. Web server logs (e.g., var/log/httpd or /var/log/apache for Apache web servers on Linux) may also record evidence of exploitation.

Review logs for SaaS services, including Office 365 and Google Workspace, to detect the configuration of new webhooks or other features that could be abused to exfiltrate data.

Addresses attack vector(s):	T1110: Brute Force, T1566: Phishing, T1133: External Remote Services, T1200: Hardware Additions, T1505: Server Software Component: SQL Stored Procedures, T1534: Internal Spearphishing, T1190: Exploit Public Facing, T1567: Exfiltration Over Web Service

STAKEHOLDERS

Executives	**IT Team**	**Legal**

By improving application log management the company can expect, increased uptime which saves money, better compliance & auditing, along with deeper insight to security issues.	Having additional information regarding application logs will give TTR & TTD.	By improving application log management the company can expect, increased uptime which saves money, better compliance & auditing, along with deeper insight to security issues.
GOALS		
Name	**Description**	**Deadline**
DS0015: Application Log Management	Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform).	Within 6 months

📊 Data Source 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	
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 Source 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	
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 Source 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	
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		

🔮 Mitigations

🔮 Preventive Mitigations:

🔮 Preventive Solution #1		
Solution #1 M1017: User Training	**Difficulty:** 1 (Easy) ▾	**Priority:** 3 (High) ▾
Train users to be aware of access or manipulation attempts by an adversary to reduce the risk of successful spearphishing, social engineering, and other techniques that involve user interaction.		
Addresses attack vector(s):	T1566: Phishing, T1036: Masquerading, T1078: Valid Accounts, T1020: Automated Exfiltration, T1528: Steal Application Access Token	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
Resolve the lack of security training by scheduling & enforcing basic cybersecurity training to increase awareness of different common threats used to attack business online. This will save the company time & ultimately money.	Security training reduces risk of incidents.	Reduces risk of breaches which helps to meet regulatory compliance.
GOALS		
Name	**Description**	**Deadline**
User Training	Our goal would be to implement quarterly cybersecurity awareness training.	The IT department should conduct demonstrations quarterly.

🔮 Preventive Solution #2		
Solution #2 M1018: User Account Management	**Difficulty:** 2 (Medium) ▾	**Priority:** 3 (High) ▾
Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting bruteforce attempts.		

Consider defining and enforcing a naming convention for user accounts to more easily spot generic account names that do not fit the typical schema. Enforce the principle of least privilege by limiting privileges of user accounts so only authorized accounts can modify and/or add server software components. Regularly audit user accounts for activity and deactivate or remove any that are no longer needed. Enforce role-based access control to limit accounts to the least privileges they require. A Cloud Access Security Broker (CASB) can be used to set usage policies and manage user permissions on cloud applications to prevent access to application access tokens. In Kubernetes applications, set "automountServiceAccountToken: false" in the YAML specification of pods that do not require access to service account tokens.		
Addresses attack vector(s):	T1110: Brute Force, T1036: Masquerading, T1505: Server Software Component: SQL Stored Procedures, T1078: Valid Accounts, T1020: Automated Exfiltration, T1528: Steal Application Access Token	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
By strengthening User Account Management, it will lower cost, increase efficiency while increasing security.	By following PoLP it will minimize potential damage from breaches. It will also help prevent human error & will prevent the spread of malware.	The company should follow PoLP guidelines & enforce things like MFA. By being PCI-DSS compliant, the company will save money & avoid fines.
GOALS		
Name	**Description**	**Deadline**
M1018: User Account Management	Manage the creation, modification, use, and permissions associated to user accounts.	2 Months

🔮 Preventive Solution #3		
Solution #3 M1016: Vulnerability Scanning	**Difficulty:** 1 (Easy) ▾	**Priority:** 3 (High) ▾
Regularly scan externally facing systems for vulnerabilities and establish procedures to rapidly patch systems when critical vulnerabilities are discovered through scanning and through public disclosure.		

Addresses attack vector(s):	T1566: Phishing, T1036: Masquerading, T1078: Valid Accounts, T1020: Automated Exfiltration, T1528: Steal Application Access Token	
STAKEHOLDERS		
Executives	**IT Team**	**Legal**
By improving vulnerability management the organization can reduce risk, minimize downtime & ensure operations of IT infrastructure.	By improving vulnerability management the organization can reduce risk, minimize downtime & ensure operations of IT infrastructure.	Lack of compliance can lead to fines. As a result, our suggestion would be to continuously scan the network & to employ a proper patch management policy. This will increase compliance & decrease the likelihood of fines.
GOALS		
Name	**Description**	**Deadline**
M1016: Vulnerability Scanning	Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them.	6 months to 1 year