

Complete the	Key Assets sheet first to pre-populate this c	Name system component here.	Classify this component of the system.	How does this attack surface involve the	Key Asset?	Does this surface connect to any other surfaces?
4.1.2	4.2.1	4.2.1	4.2.1	4.2.1	4.2.1	4.2.1
Key Assets	Attack Surface	Component type	Relationship			Related surfaces
Intellectual property (IP): proprietary game source code.	Github	Software	software used to manage the source code			Game and API source code, Developers, Workstation
Intellectual property (IP): proprietary game source code.	Game and API source code	Data	Game and API code			Github, Developers, Workstation
Intellectual property (IP): proprietary game source code.	Developers	People	Developers have access to the source code			Game and API source code, Github, Workstation
Intellectual property (IP): proprietary game source code.	Workstation	Hardware	May have source code and game design			Developers, Game and API source code, Github
Payment information of users for billing (paid subscriptions).	Network traffic	Data	Network security vulnerabilities may be used to gain access			Workstation, Developers, Credit card information, Employees, Game and API source code
Payment information of users for billing (paid subscriptions).	Credit card information	Data	Credit card information can be used or sold			Endpoint devices, Network traffic, Workstation, Developers, Game and API source code, Github
Payment information of users for billing (paid subscriptions).	Financial management software	Software	Financial management software used to gain financial information			Developers, Workstation, Network traffic, Credit card information, Employees, Endpoint devices
Payment information of users for billing (paid subscriptions).	Employees	People	Employees have access to financial information			Workstation, Credit card information, Network traffic, Endpoint devices
In-game private chat system (features end-to-end encryption; some interesting research regarding this).	Endpoint devices	Hardware	Endpoints can open access to users			End users, Analytics data, Security tools
In-game private chat system (features end-to-end encryption; some interesting research regarding this).	End users	People	Users may be potential target			Github, Game and API source code, Developers, Network traffic, Employees, Endpoint devices, Analytics data, Servers
In-game private chat system (features end-to-end encryption; some interesting research regarding this).	Chat messages	Data	Data may have vital user information			End users, Endpoint devices, Employees, Credit card information, Servers, Game and API source code
In-game private chat system (features end-to-end encryption; some interesting research regarding this).	Message system	Software	Security breachment to gain access unnoticed			Servers, IT administrators, End users, Endpoint devices, Network traffic, Github, Analytics data
Personally identifiable information(PII)	Third party contractors	People	Third party contractors may be used to gain access			Game and API source code, Developers, Workstation, Network traffic, Credit card information, Employees, Analytics data, Servers
Personally identifiable information(PII)	Storage devices	Hardware	Storage devices contain PII			Game and API source code, Developers, Workstation, Network traffic, Employees, Analytics data, Security tools
Personally identifiable information(PII)	Employees	People	IT administrators have access to PII			Developers, Workstation, Network traffic, Endpoint devices, Security tools, Analytics data, Servers, Storage devices
Personally identifiable information(PII)	End Users	People	End users			
Personally identifiable information(PII)	Credentials database and information	Data	Credentials database/ information used to exploit end user and employees			

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]