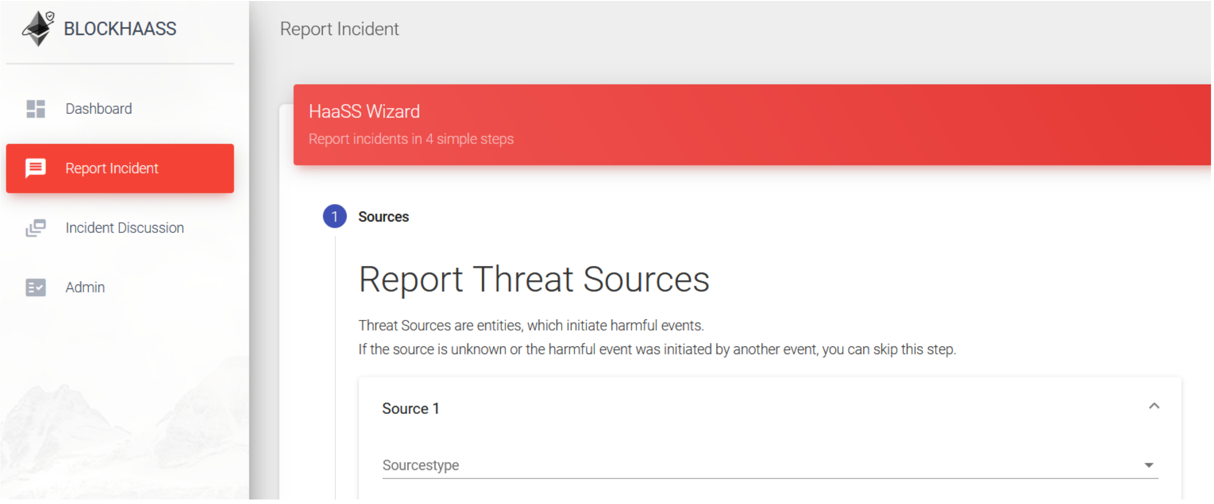
Universität Regensburg

Evaluation “BISCUIT - Blockchain Security Incident Reporting and Discussion based on Human Observations”

First off, thank you sincerely for agreeing to participate in our short interview. The goal of our research is to create a way for **users to report blockchain security incidents**. We have created a wizard and taxonomy for these incidents, which we would like to test together with you. We have chosen you since **you have gained prior knowledge with blockchain as part of your studies** and thus fit our definition of a security novice.

The purpose of this interview is to verify the suitability of our interactive wizard for reporting incidents. You will be given a series of case descriptions, which you are asked to enter in our wizard.



Threat Sources are entities, which initiate harmful events.
If the source is unknown or the harmful event was initiated by another event, you can skip this step.

As Event Type you can generally select

Attack > **Nefarious activity / Abuse**

For example, for reentrancy attack you may select

Attack > **Nefarious activity / Abuse** > **Unauthorized activities** > **Unauthorized code execution** > **Reentrancy**

Context 1 – Permissioned Blockchains

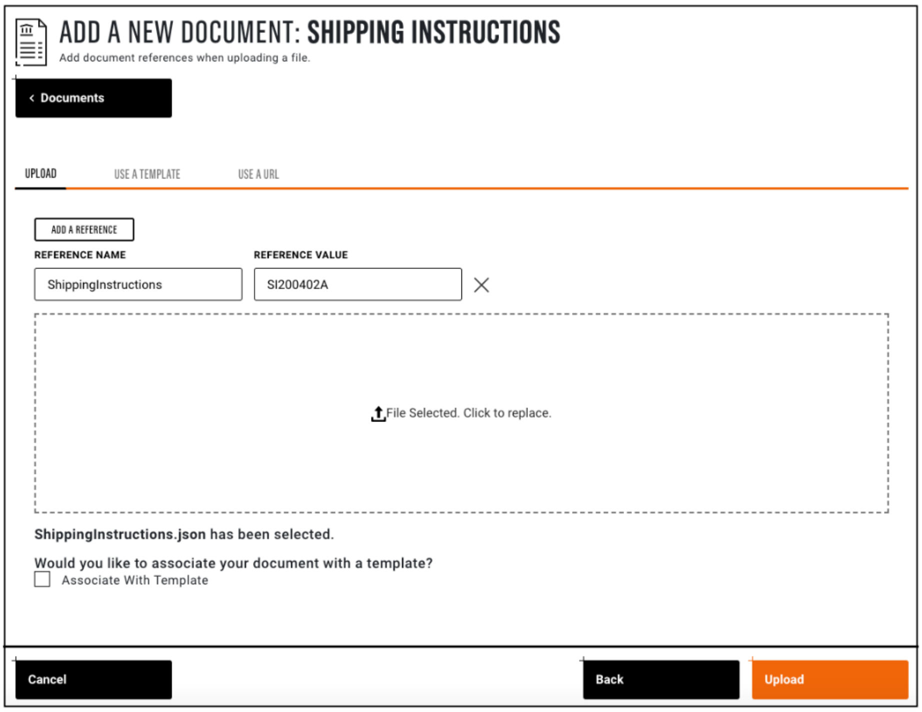
You are participating in a Container tracking blockchain. You are trying to update a container shipment on the blockchain by adding tracking information for its onward transport.

For this purpose, you want to upload a new document. However, there are some issues. Please create a new incident in BISCUIT for each issue.

a) You cannot reach the website for 5 minutes.

b) Afterwards, when viewing your documents, you notice that some documents are missing which you didn't remove. You remember that earlier you received an email asking you to update your credential information for the blockchain application, which seemed unusual. Despite some initial suspicion you went ahead and entered your credentials after following the link. You suspect that your identity has been compromised."

c) After your identity has been restored, you can now upload the document. However, afterwards you notice that the change is not persisted in the main document overview. It seems your transaction was not processed by the blockchain. You suspect an issue with the consensus algorithm.



ADD A NEW DOCUMENT: **SHIPPING INSTRUCTIONS**

Add document references when uploading a file.

REFERENCE NAME	REFERENCE VALUE
ShippingInstructions	SI200402A

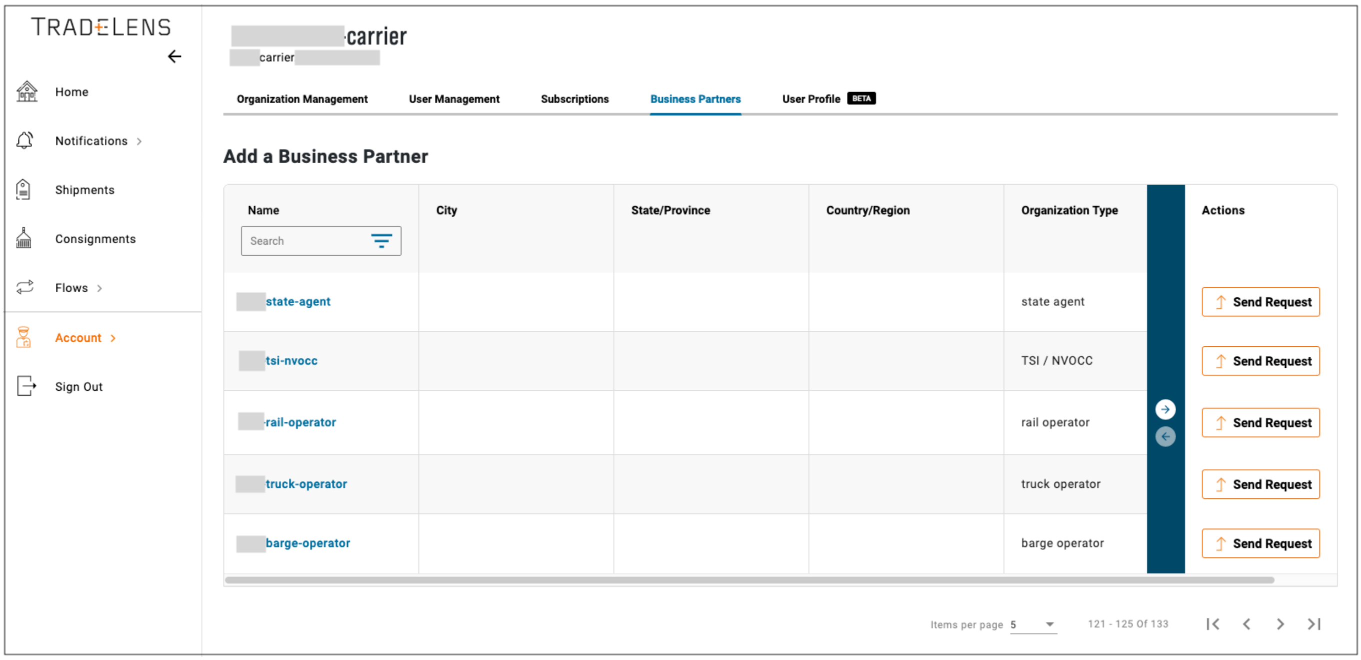
File Selected. Click to replace.

ShippingInstructions.json has been selected.

Would you like to associate your document with a template?

□ Associate With Template

d) When viewing your business partners, you notice that there are several identities that should not exist. You have never done business with truck-operator or barge-operator. For this reason, you suspect a sybil attack, where one of the network operators is creating fake identities.



[redacted]-carrier

[redacted] carrier [redacted]

Add a Business Partner

Name Search	City	State/Province	Country/Region	Organization Type	Actions
[redacted]state-agent				state agent	Send Request
[redacted]tsi-nvocc				TSI / NVOCC	Send Request
[redacted]-rail-operator				rail operator	Send Request
[redacted]truck-operator				truck operator	Send Request
[redacted]barge-operator				barge operator	Send Request

Items per page 5   121 - 125 Of 133

Context 2 – Permissionless Blockchains

Please take a look at the following suspicious accounts on Etherscan.

https://etherscan.io/address/0x14EC0cD2aCee4Ce37260b925F74648127a889a28

https://etherscan.io/address/0xcE1F4B4F17224ec6df16Eeb1e3e5321c54Ff6EDe
transaction 0x0016745693d68d734faa408b94cdf2d6c95f511b50f47b03909dc599c1dd9ff6

Here are some pointers to look for on the transactions. Feel free to add your own observations in the description field of the report.

Call by contract. The application smart contract is called through a dedicated attacker smart contract created by the attacker. One attack example where attackers use a smart contract is the reentrancy attack.

Flash loan. While flash loans have legitimate usage for arbitrage and reducing transaction fees, they are also often used as part of attacks that try to manipulate contract logic.

Transaction frequency spike. Attackers often perform many transactions within a short period of time.

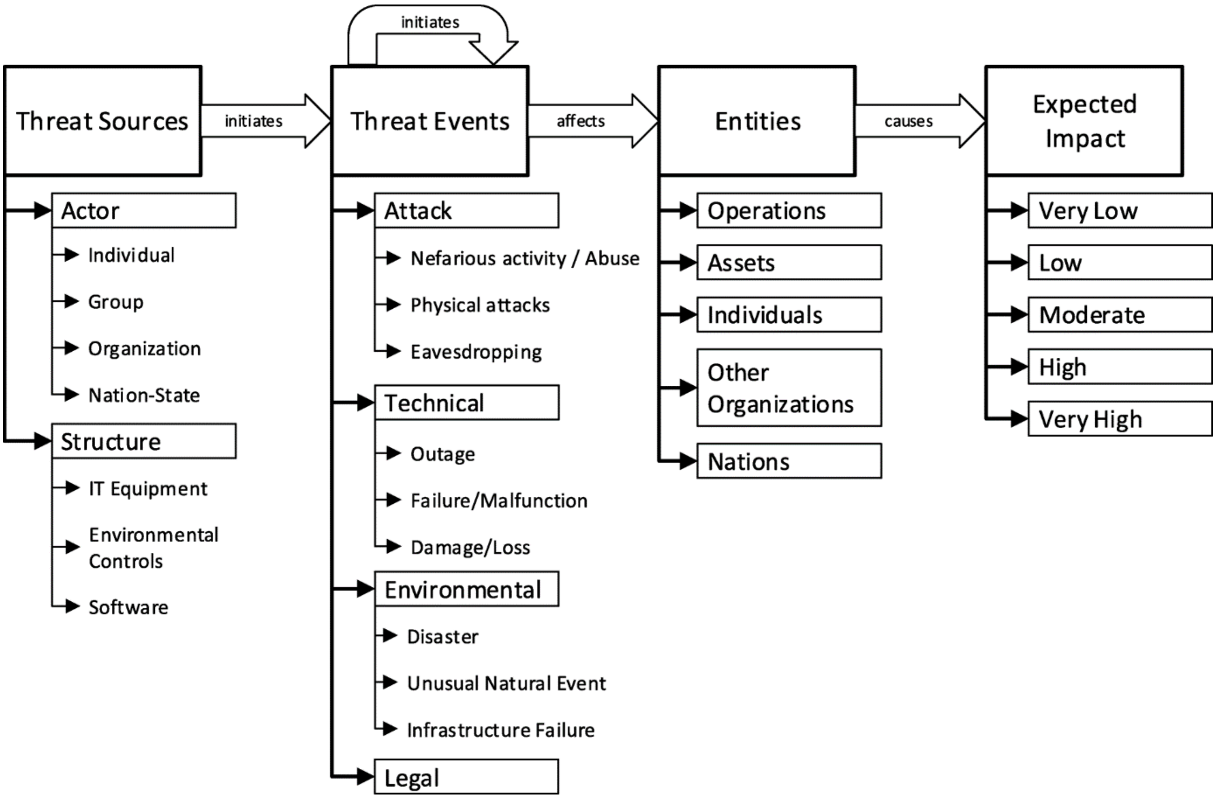
Failed transactions. Failed transactions targeting the same contract. Attackers may attempt the same attack with similar parameters multiple times.

Account creation date. Attackers usually create new accounts for attacks, so transactions made by accounts created on the same day are more likely to be used in an attack.

Gas usage. Attack transactions often come with high gas usage (for maximum impact) and/or high gas prices (for fast execution).

Tornado.Cash. The coin mixing service Tornado.Cash is popular among attackers for its ability to hide coin flows if executed correctly. If used after an attack transaction it may indicate an attempt to launder coins.

Additional information regarding our taxonomy of blockchain security incidents


initiates
Threat Sources
initiates
Threat Events
affects
Entities
causes
Expected Impact
Actor
Individual
Group
Organization
Nation-State
Structure
IT Equipment
Environmental Controls
Software
Attack
Nefarious activity / Abuse
Physical attacks
Eavesdropping
Technical
Outage
Failure/Malfunction
Damage/Loss
Environmental
Disaster
Unusual Natural Event
Infrastructure Failure
Legal
Operations
Assets
Individuals
Other Organizations
Nations
Very Low
Low
Moderate
High
Very High