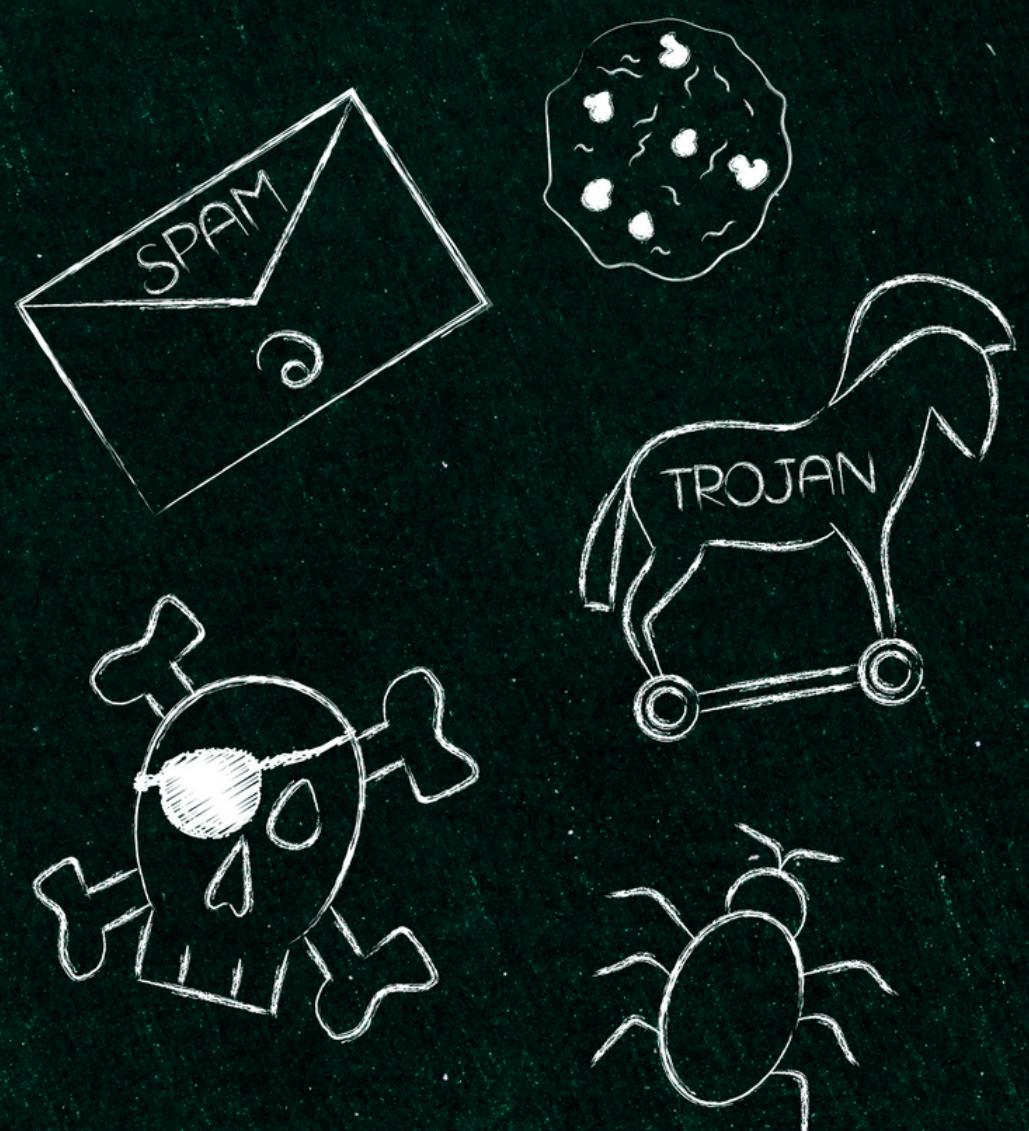
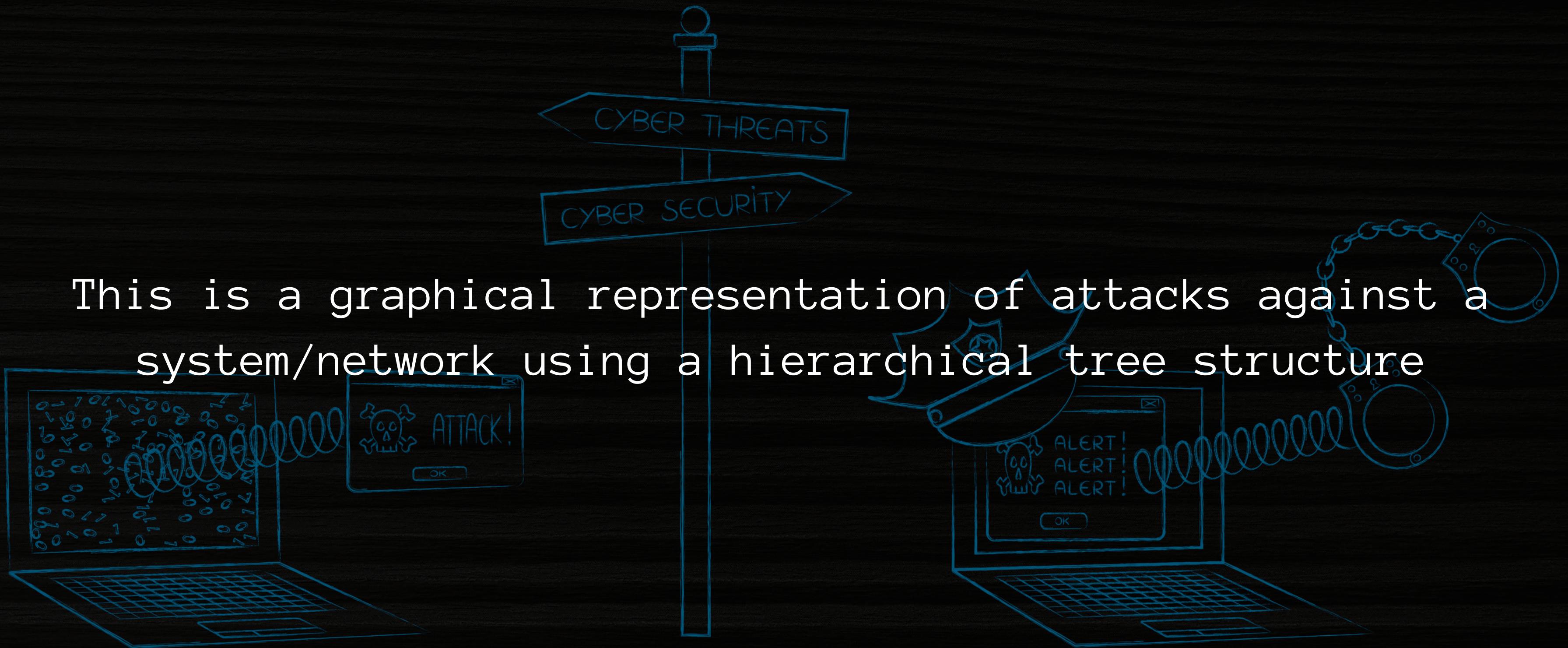


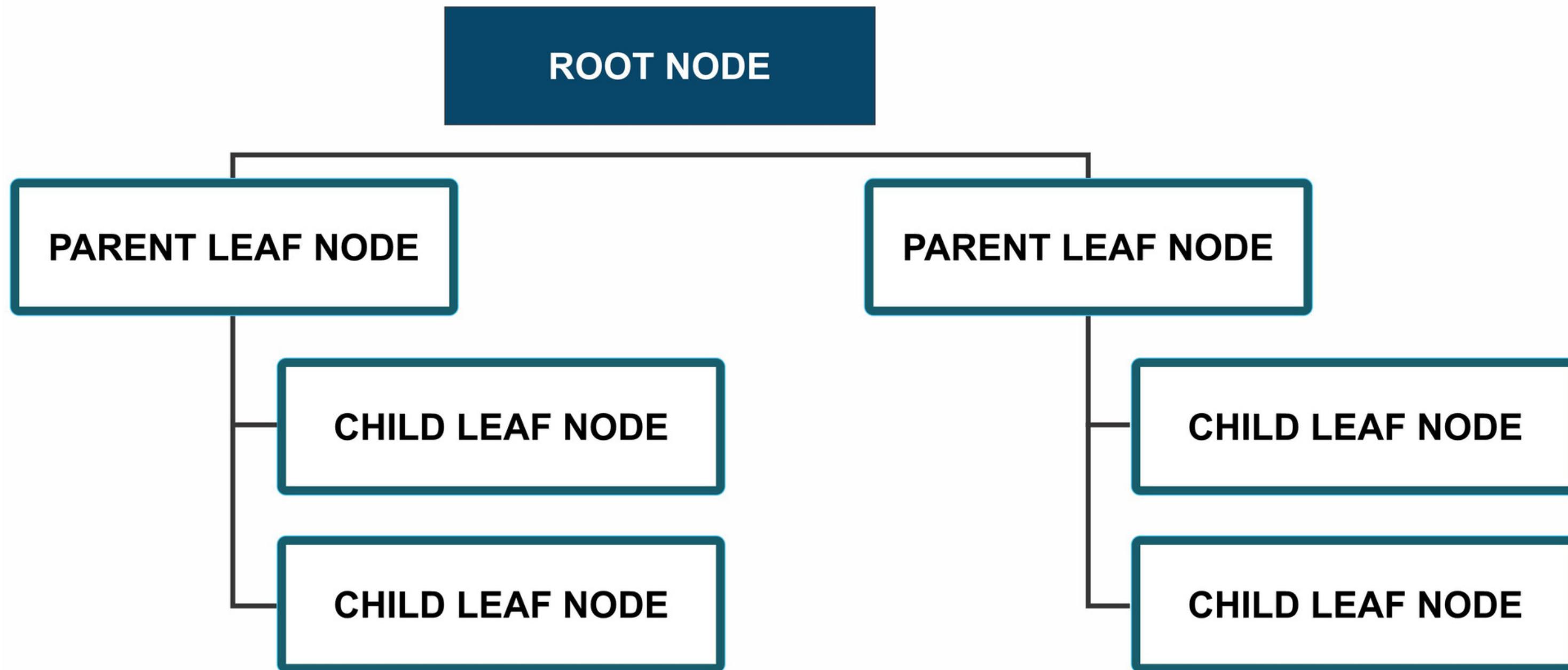
# ATTACK TREES



# What is an Attack Tree?



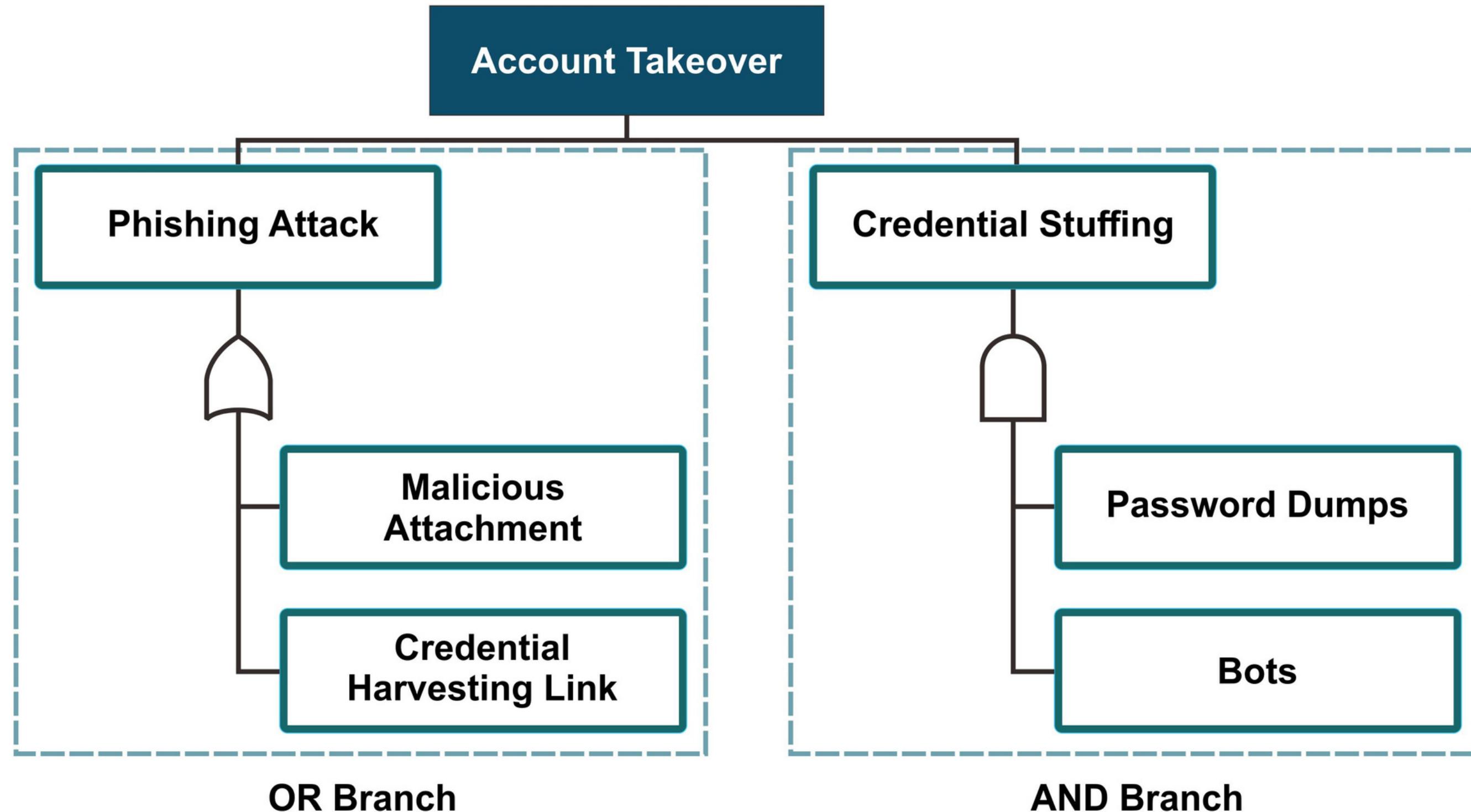
# What is an Attack Tree?



- Root node represents an objective of the attacker
- Leaf nodes represent the ways to achieve the objective



# What is an Attack Tree?



- AND trees (when all child leaf nodes must be true)
- OR trees (when any child leaf node can be true)

# Attack Tree Process

- Define the root node - The attacker's core objective
- Is it an AND, OR or a combination of both tree types
- Define the leaf nodes and child leaf nodes if available
  - Delete any unlikely/unrealistic leaf nodes
  - Check for completeness



# Attack Tree Example

Your company is on the verge of releasing a revolutionary product and are concerned that the software used to create it will either be stolen and sold to rival companies or could be used to hold the company to ransom.

A third party software development company was also involved in the development of this product



```
import _debounce from 'lodash.debounce';
import PropTypes from 'prop-types';
import React from 'react';
import cls from 'classnames';
import { withTranslation } from 'react-i18next';
```

```
import { Loading } from '@/components/ui';
import { DOCUMENT_NODE_FUNCTIONS } from '@/utils';
```

```
const DISTANCE = 20;
const DEBOUNCE_TIME = 400;
```

```
class WithInfiniteScroll extends React.Component {
```



# Attack Tree Example

Your company has so far implemented the following security controls:

- Awareness training for Phishing attacks
- Strong authentication and authorization tools
- Effective auditing and logging processes.

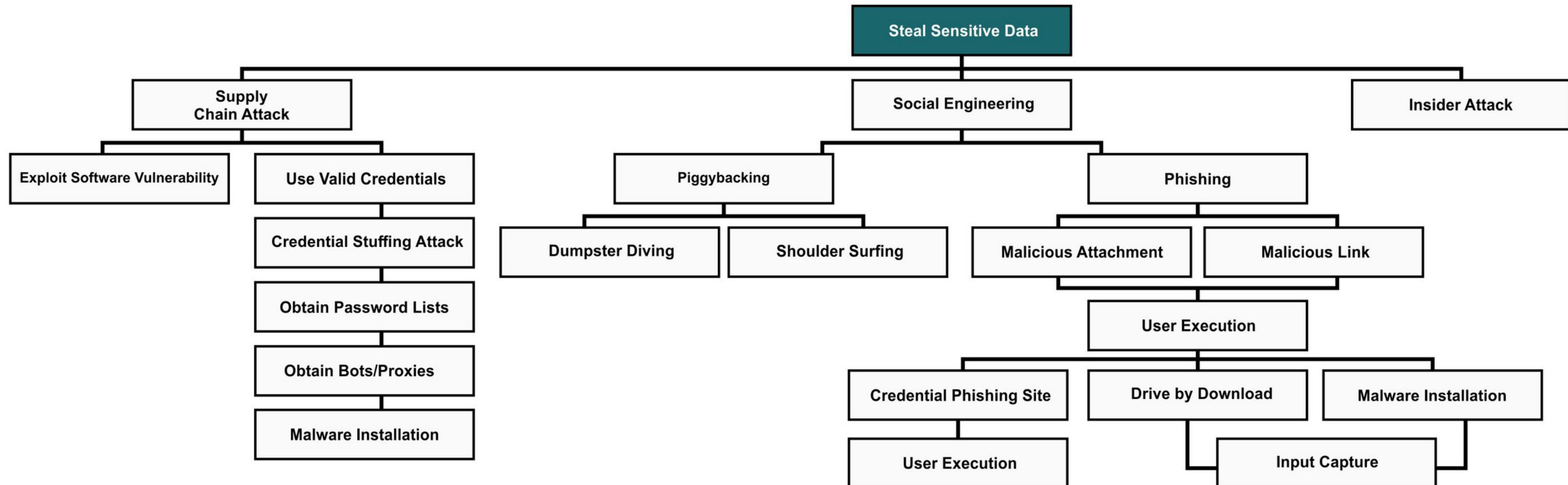


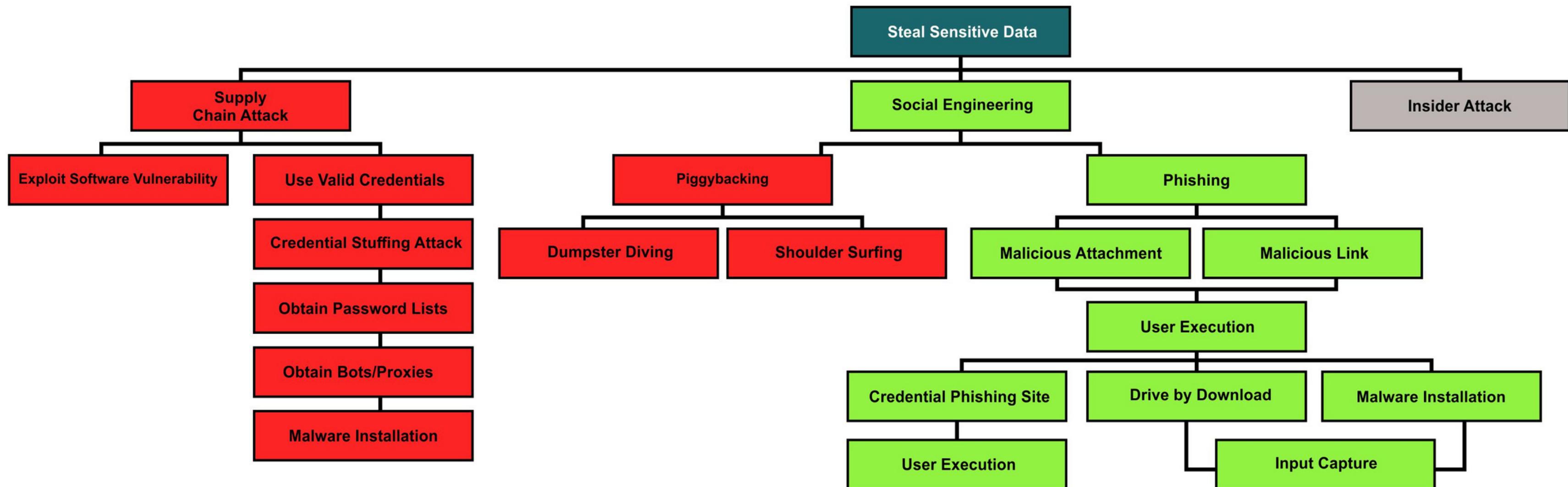
```
import _debounce from 'lodash.debounce';
import PropTypes from 'prop-types';
import React from 'react';
import cls from 'classnames';
import { withTranslation } from 'react-i18next';

import { Loading } from '@/components/ui';
import { DOCUMENT_NODE_FUNCTIONS } from '@/utils';

const DISTANCE = 20;
const DEBOUNCE_TIME = 400;
```







Most likely attack paths,  
but mitigation exists

Possible attack path,  
inadequate mitigation

Possible attack paths,  
unknown mitigation

