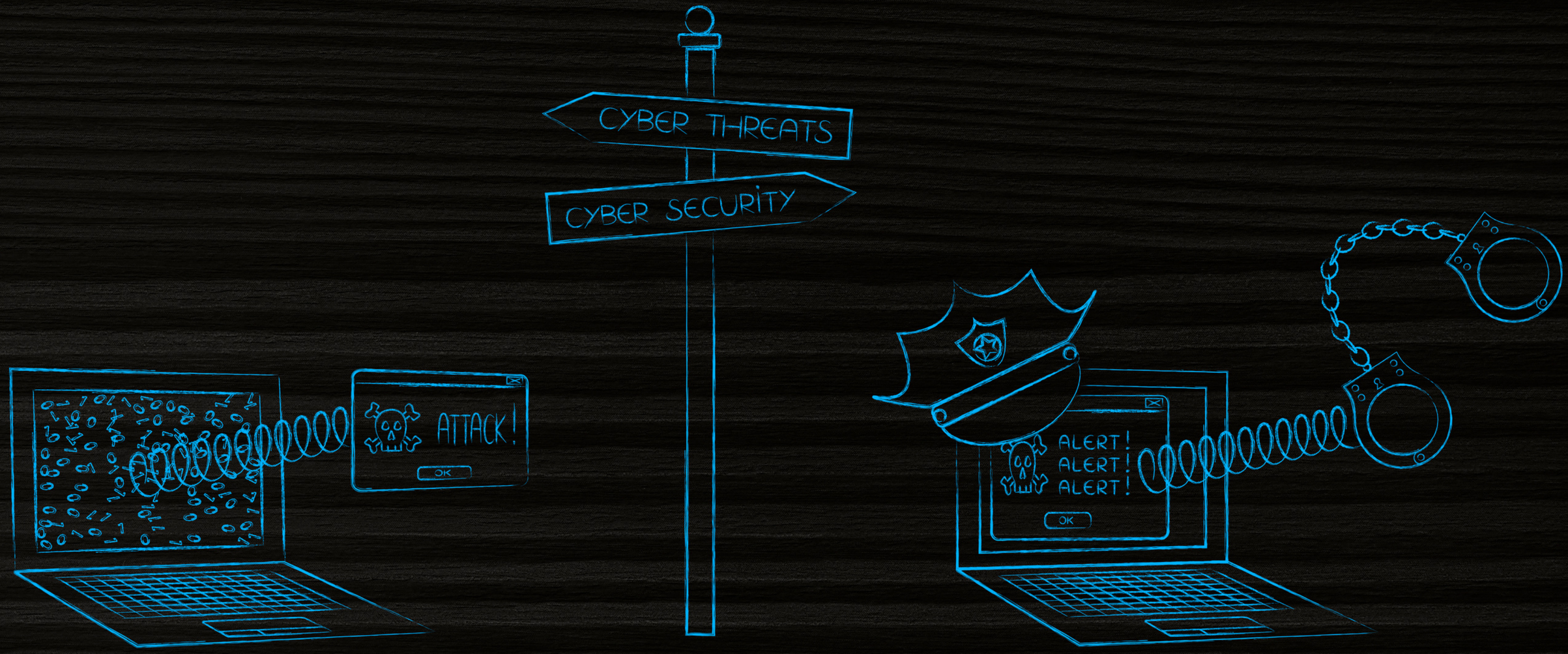
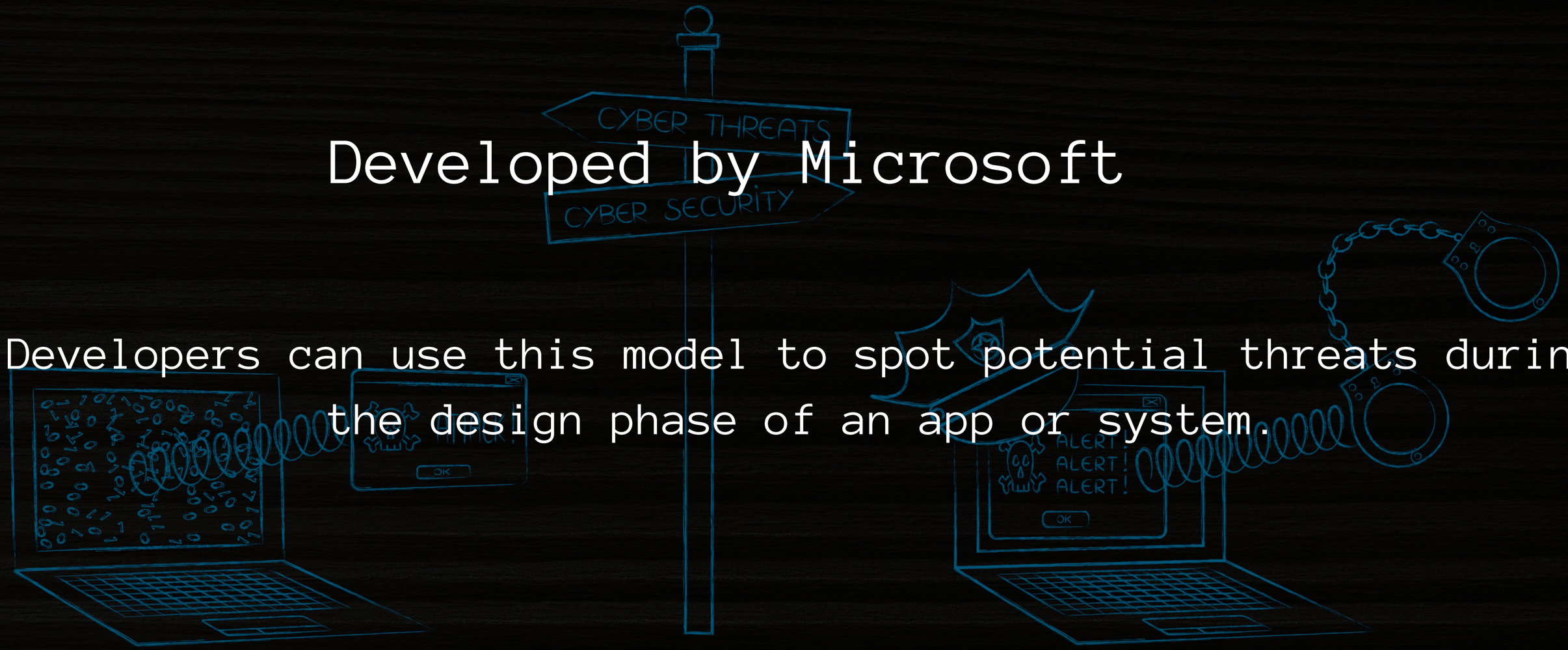
STRIDE


CYBER THREATS
CYBER SECURITY
ATTACK!
OK
ALERT!
ALERT!
ALERT!
OK

STRIDE

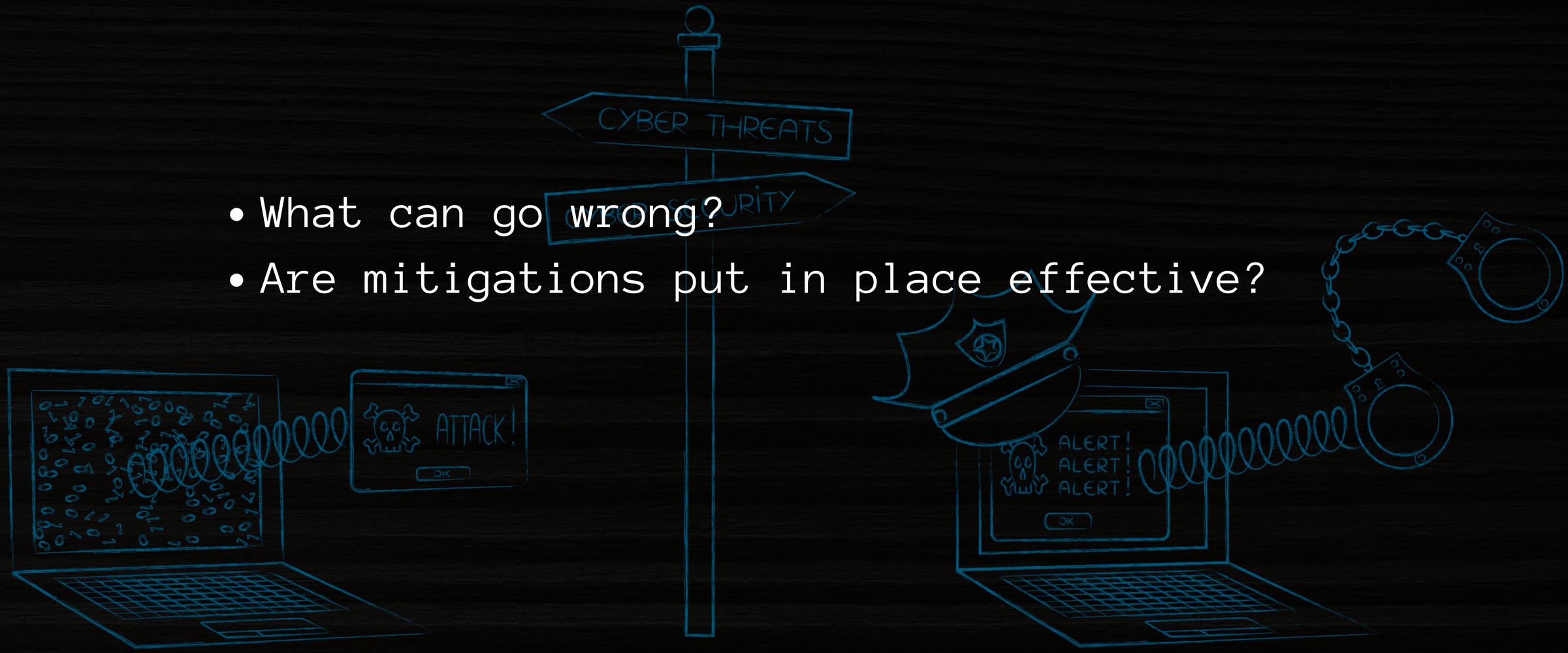


Developed by Microsoft

Developers can use this model to spot potential threats during the design phase of an app or system.

STRIDE

- What can go wrong?
- Are mitigations put in place effective?



STRIDE

- S – Spoofing / Authentication
- T – Tampering / Integrity
- R – Repudiation / Non Repudiation
- I – Information Disclosure / Confidentiality
- D – Denial of Service / Availability
- E – Escalation of Privileges / Authorization

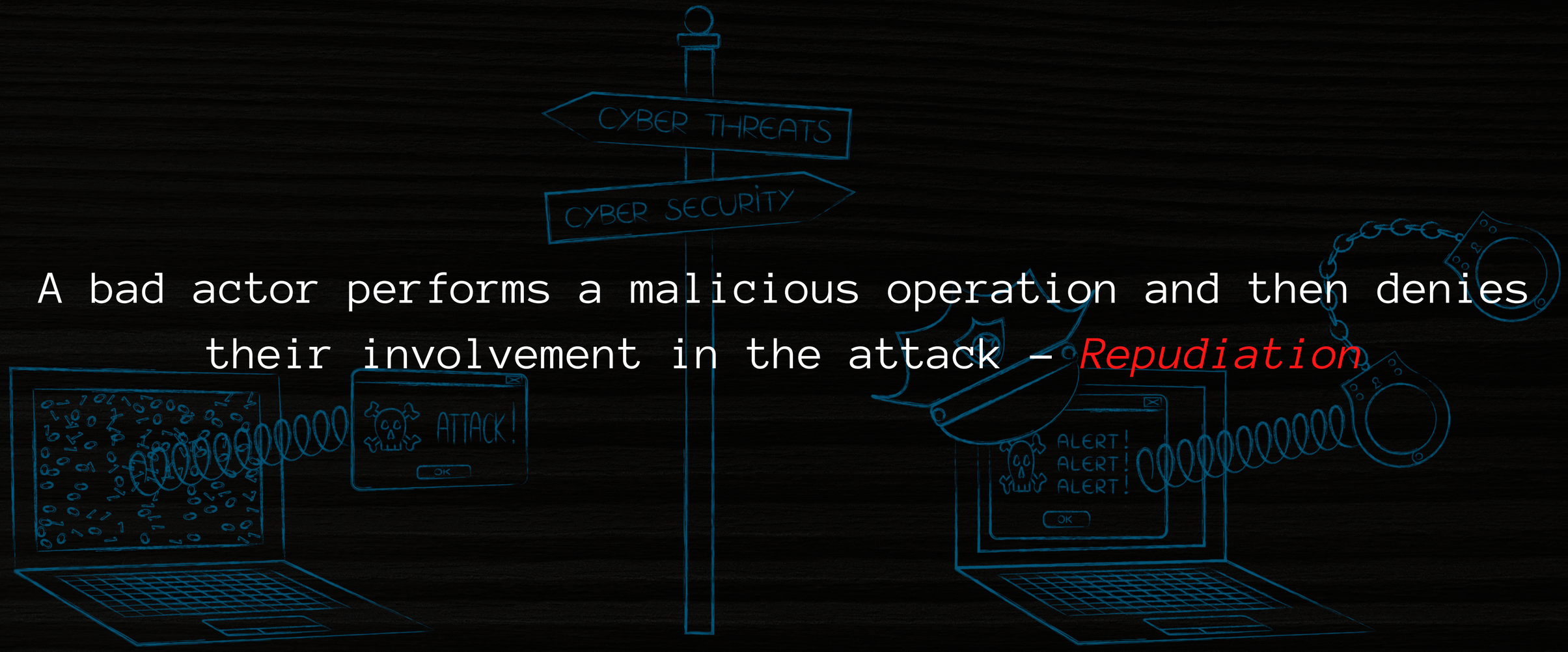
STRIDE

A hacker fakes their identity and gains access – *Spoofing*

STRIDE

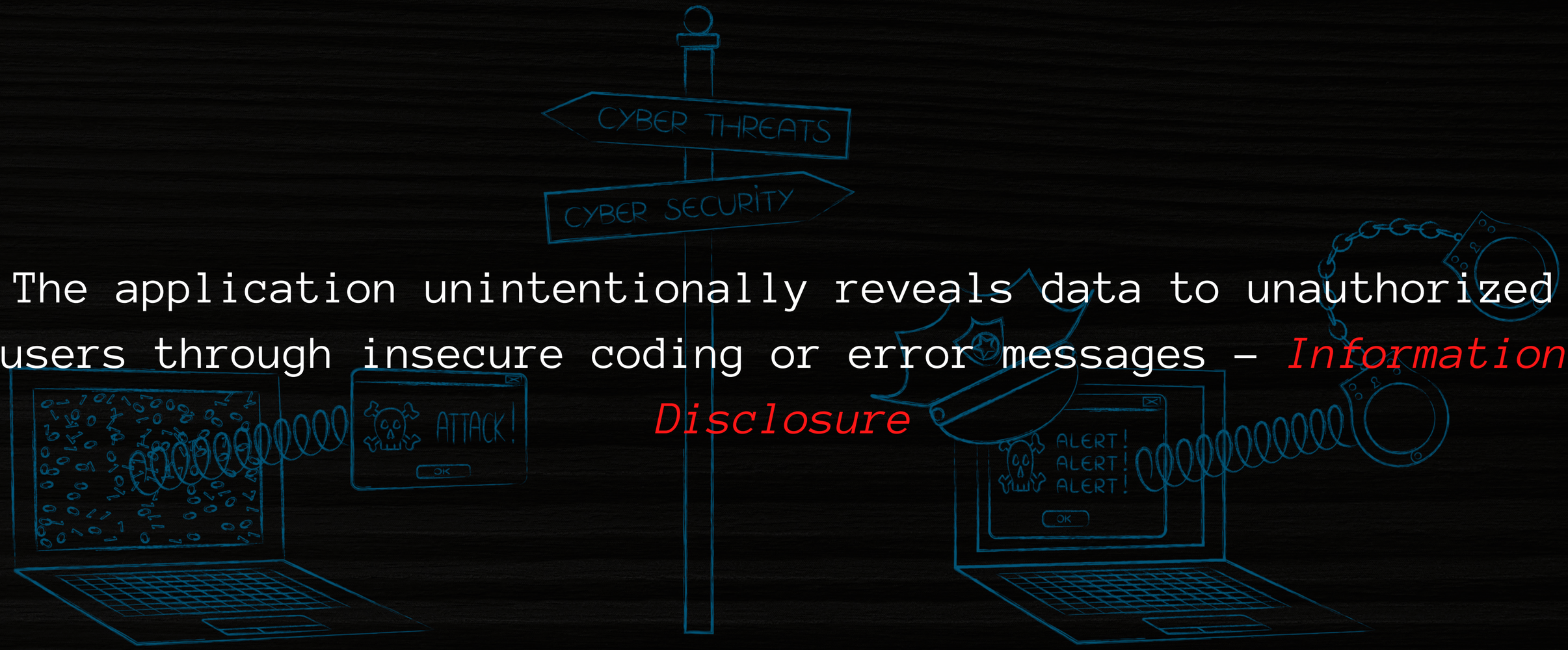
A disgruntled employee can tamper with company data by changing the software code – *Tampering*

STRIDE



A bad actor performs a malicious operation and then denies their involvement in the attack – *Repudiation*

STRIDE

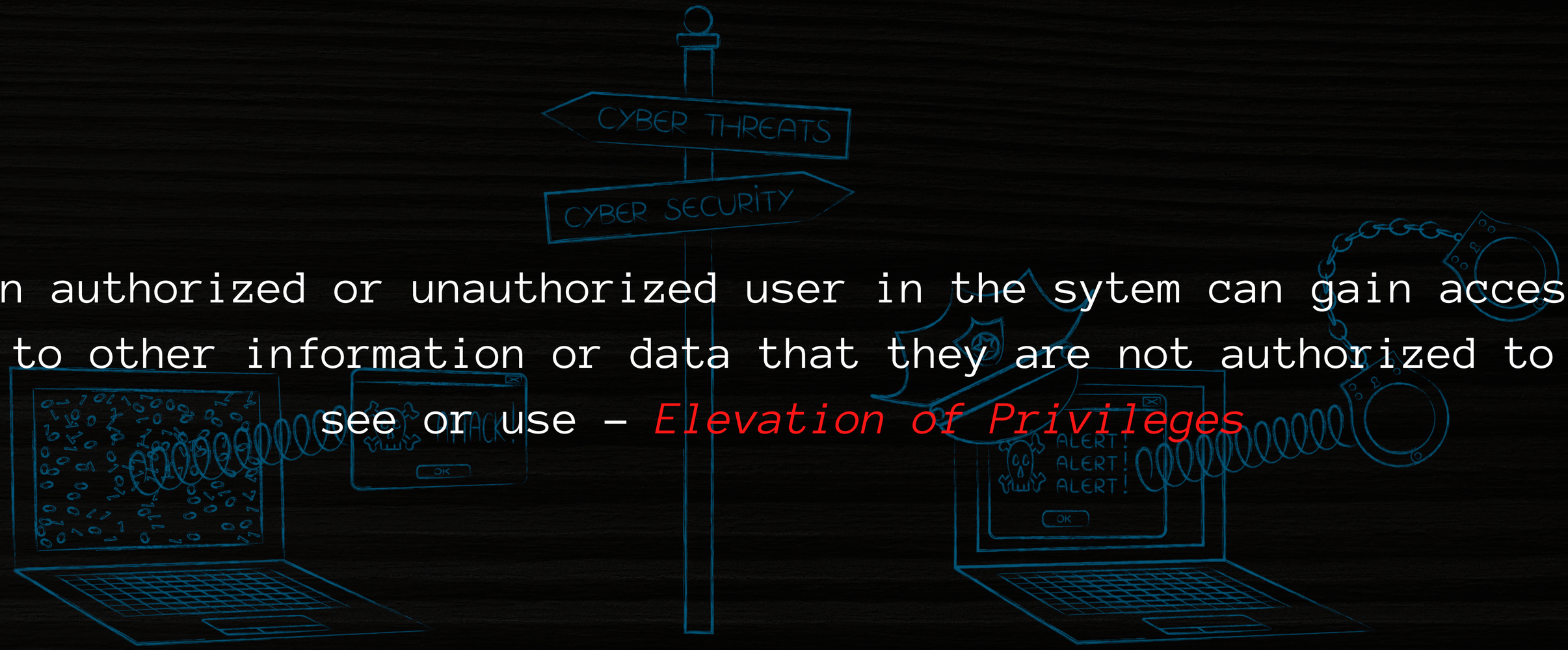


The application unintentionally reveals data to unauthorized users through insecure coding or error messages – *Information Disclosure*

STRIDE

DoS attacks restrict an authorized user from accessing the applciation – *Denial of Service*

STRIDE



An authorized or unauthorized user in the sytem can gain access to other information or data that they are not authorized to see or use – *Elevation of Privileges*

STRIDE

All possible threats are enumerated and then addressed

STRIDE

Threats are addressed by:

- Mitigation
- Elimination (component is removed)
- Transferred
- Accepted

STRIDE

Final step is to validate the model through testing for completeness, accuracy and effectiveness.