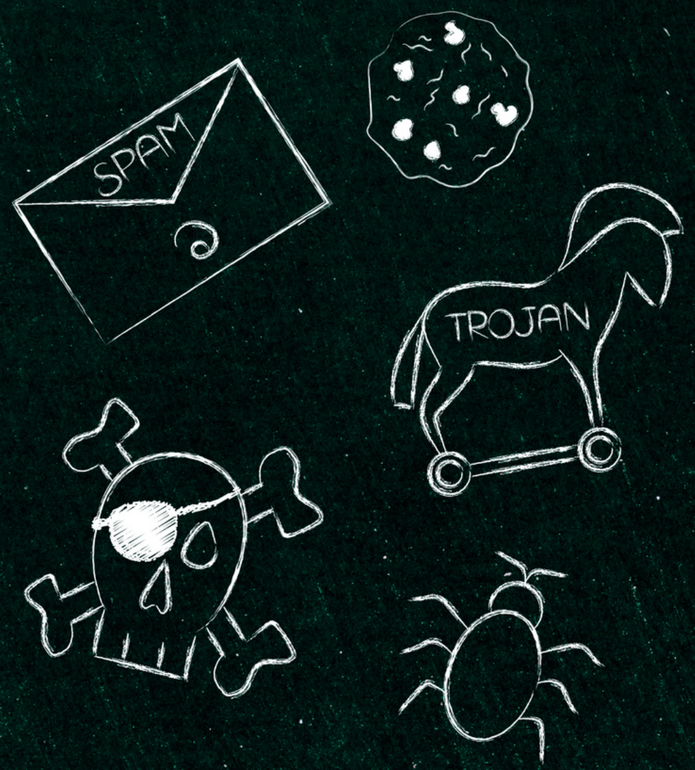
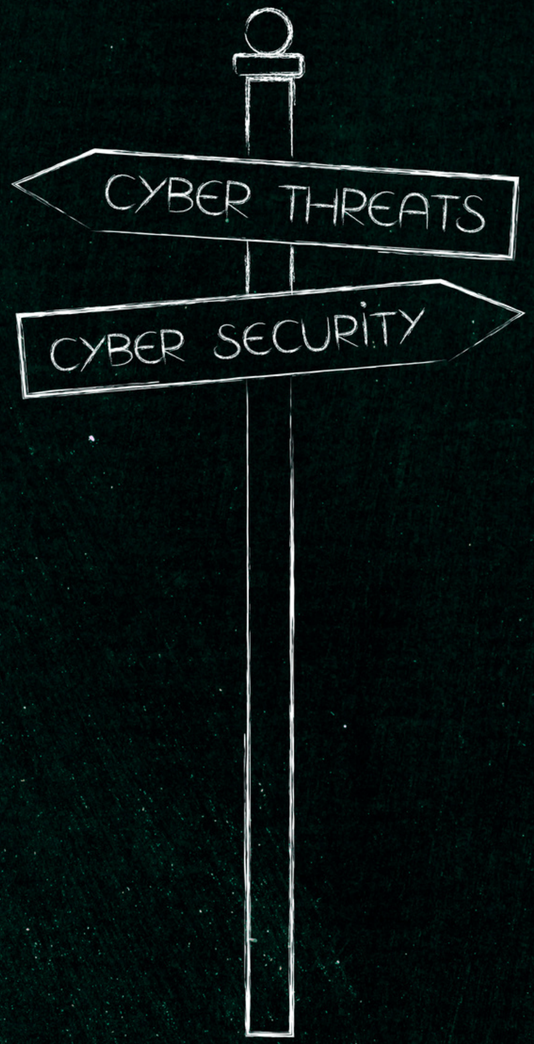
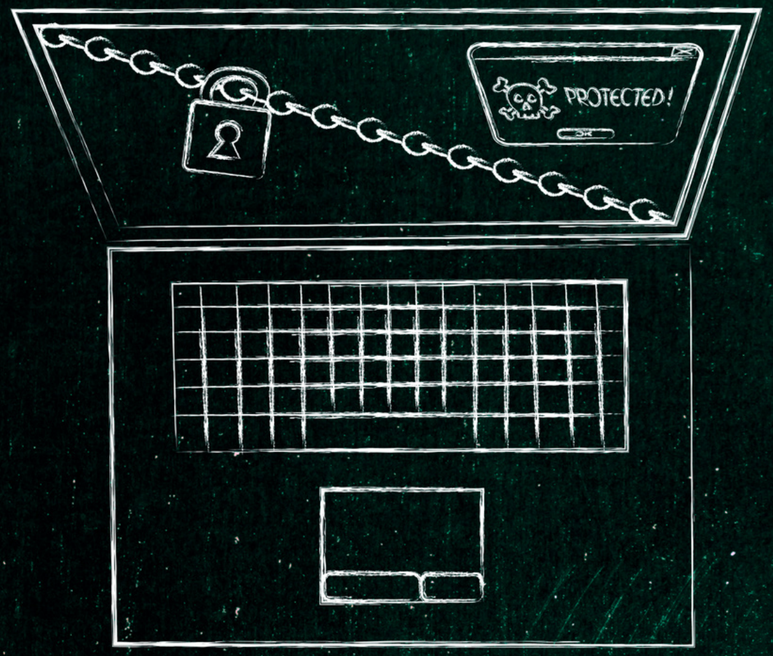
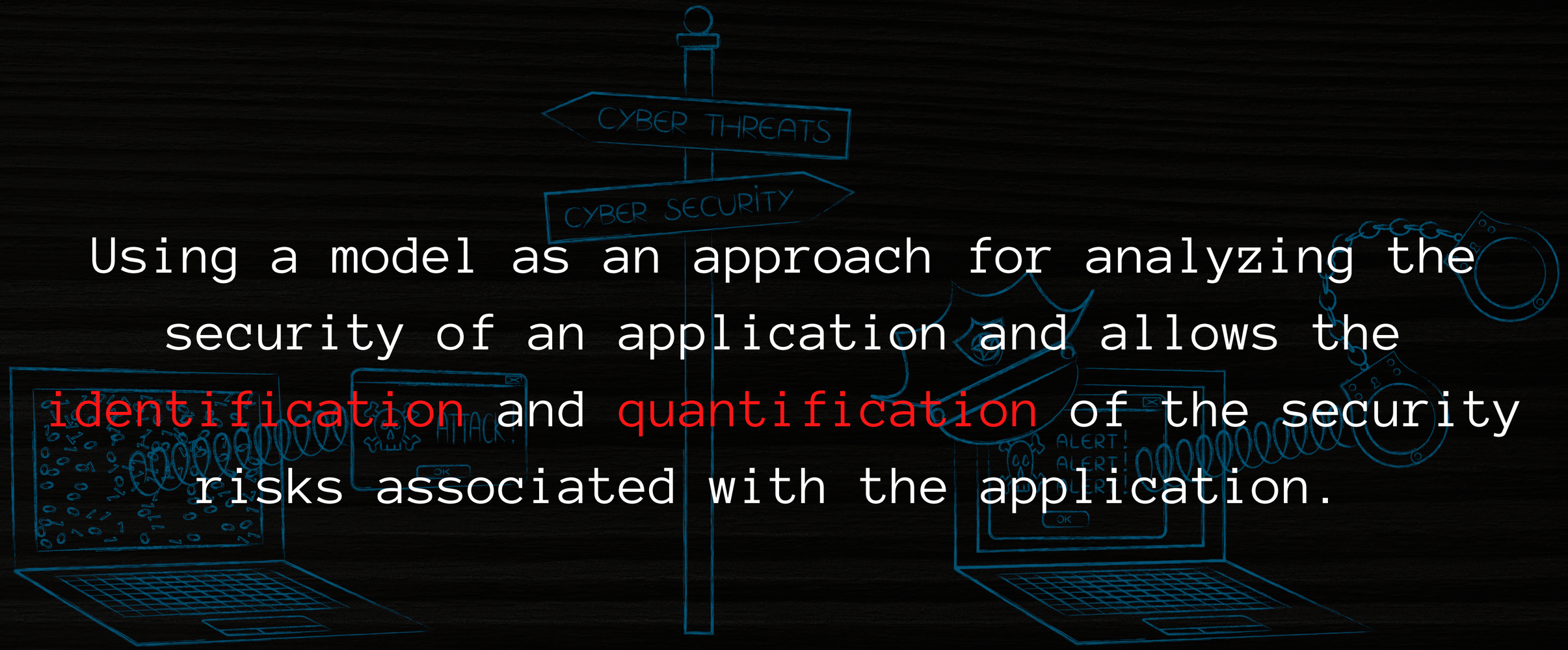






THREAT MODELLING

What is Threat Modelling?



Using a model as an approach for analyzing the security of an application and allows the identification and quantification of the security risks associated with the application.

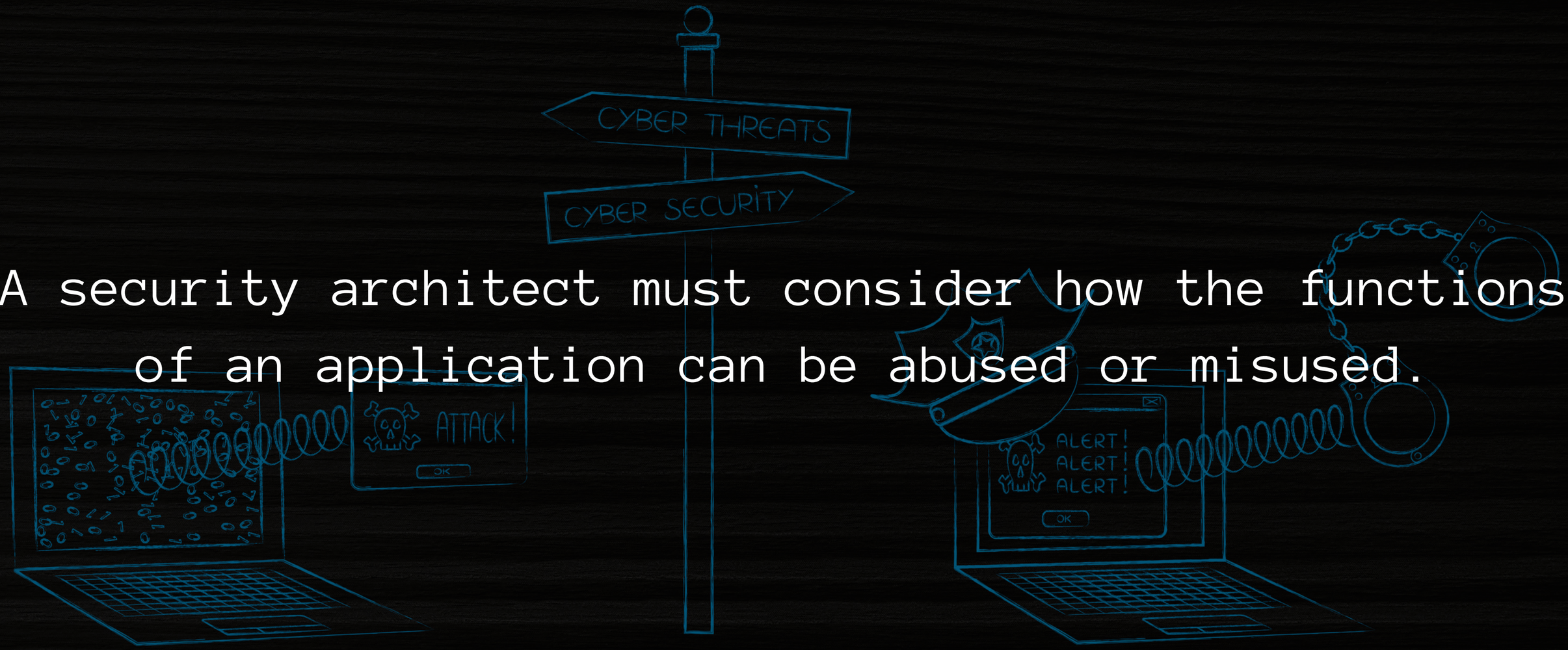
Threat Modelling Methodologies

- STRIDE
- DREAD
- PASTA
- TRIKE
- VAST
- OCTAVE
- PnG

Threat Modelling Perspectives

- Functional
- Process
- Deployment
- Data Flows
- Social
- Environmental

Abuse/Misuse Case



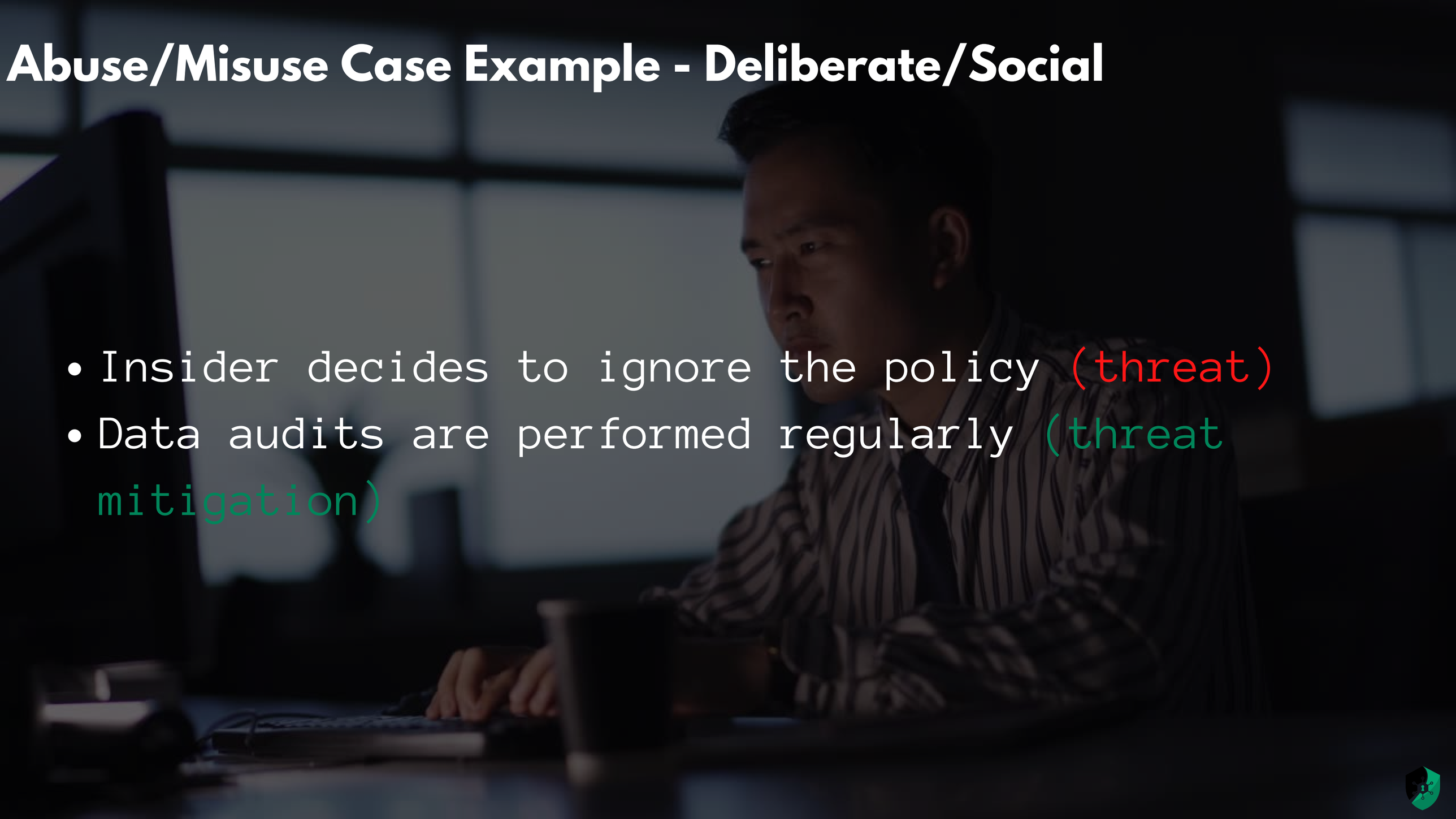
A security architect must consider how the functions of an application can be abused or misused.

Abuse/Misuse Case Example - Deliberate/Social

Sensitive company data must not be copied to personal USB drives (threat)

Use of security policy banning the use of USB drives (threat mitigation)

Abuse/Misuse Case Example - Deliberate/Social

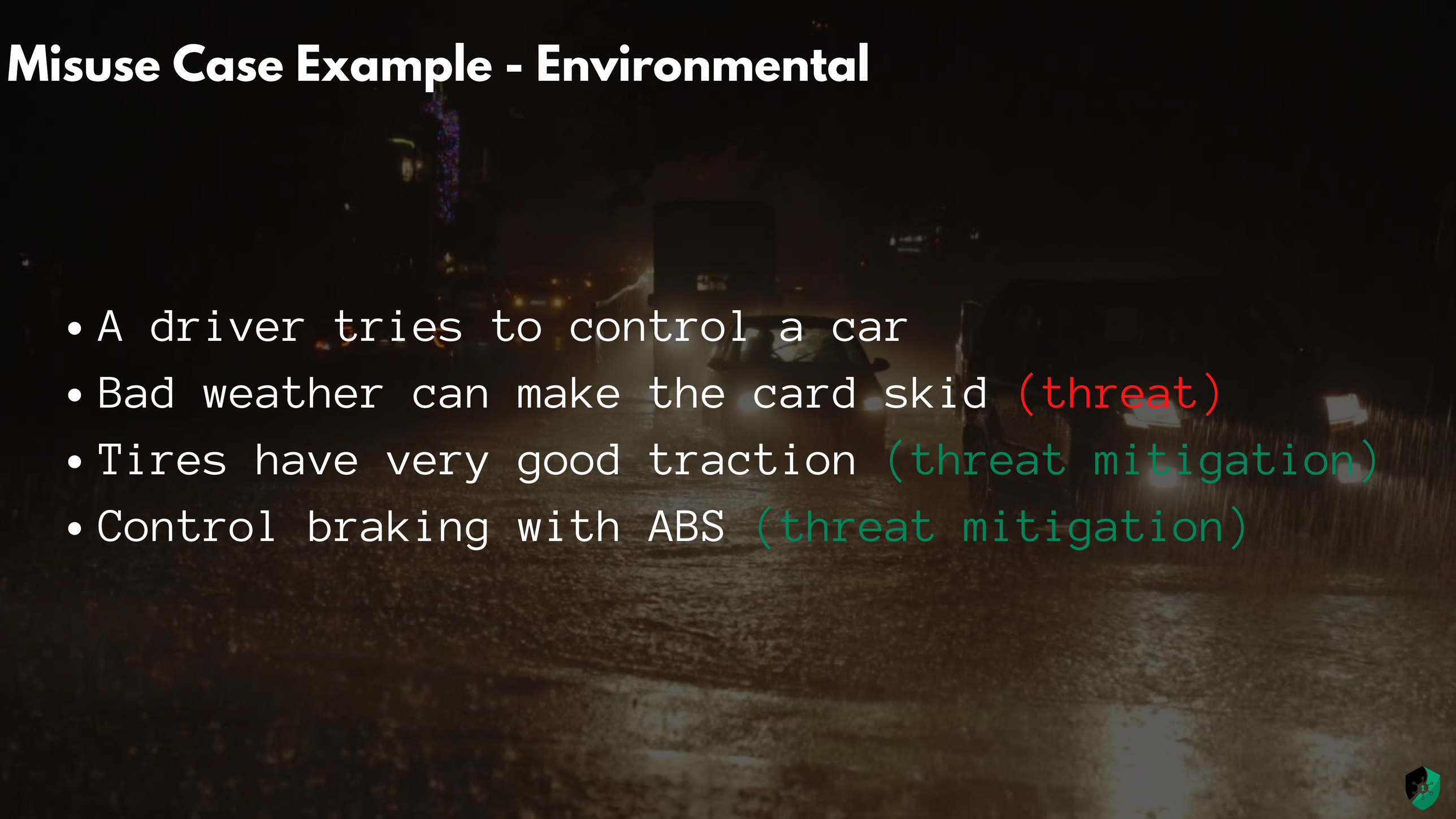


- Insider decides to ignore the policy (threat)
- Data audits are performed regularly (threat mitigation)

Abuse/Misuse Case Example - Deliberate/Social

- What if the audit fails (threat)?
- USB drives are disabled (threat mitigation)

Misuse Case Example - Environmental



- A driver tries to control a car
- Bad weather can make the card skid (threat)
- Tires have very good traction (threat mitigation)
- Control braking with ABS (threat mitigation)