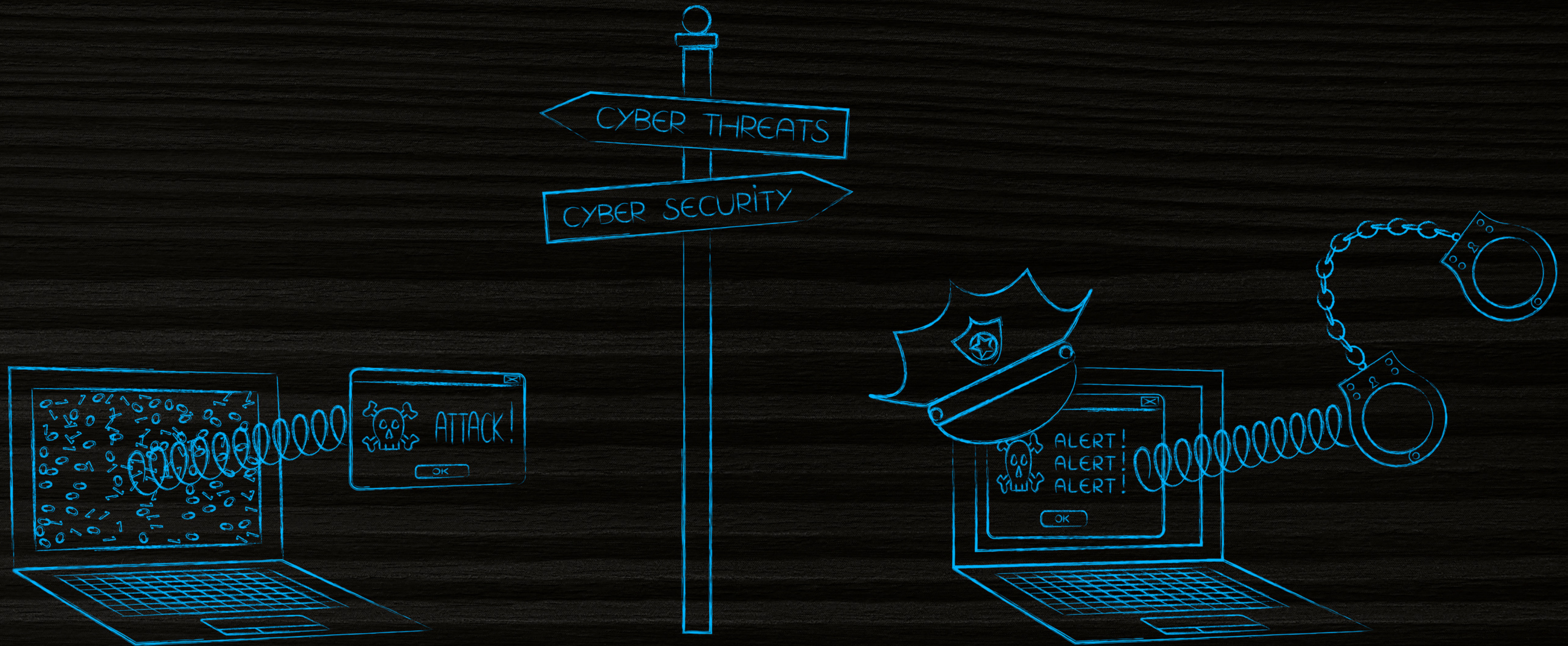


# OCTAVE





# OCTAVE

Operationally Critical Threat, Asset & Vulnerability Evaluation





# OCTAVE

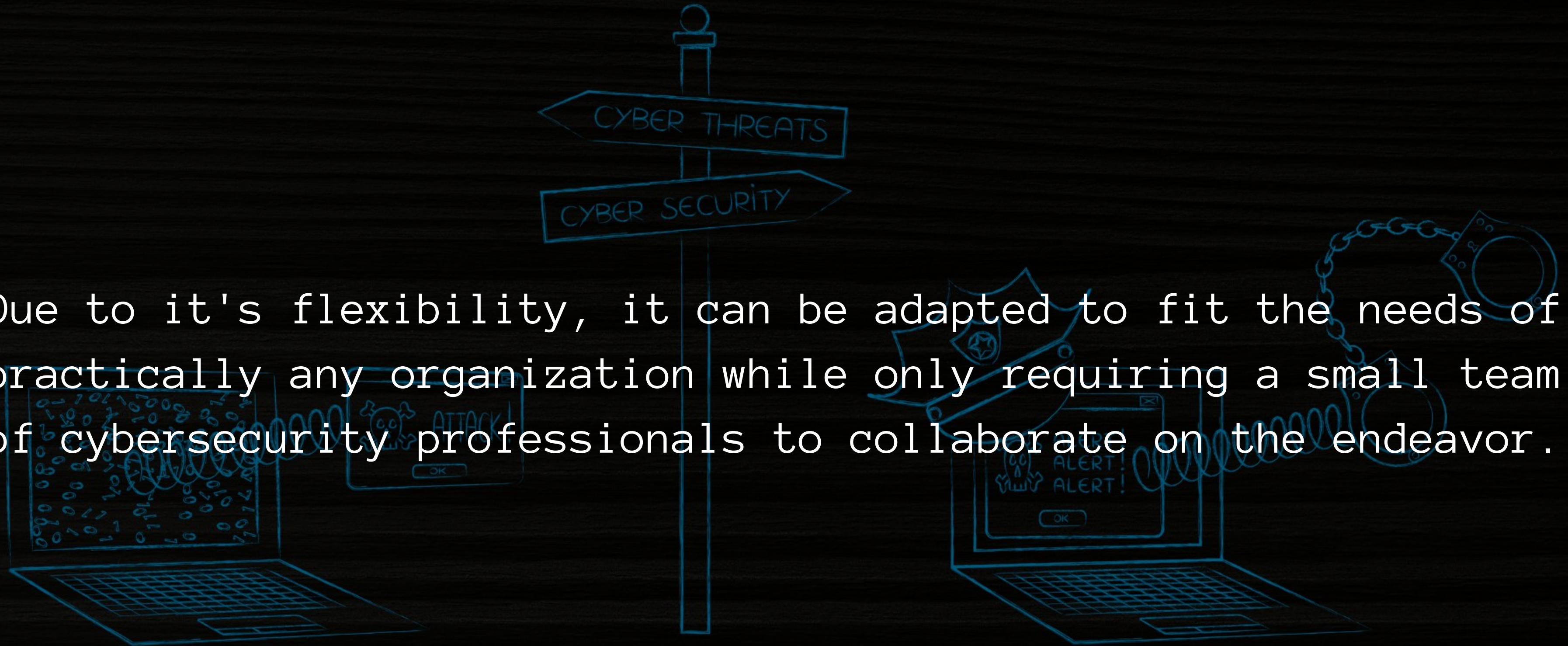
is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy





# OCTAVE

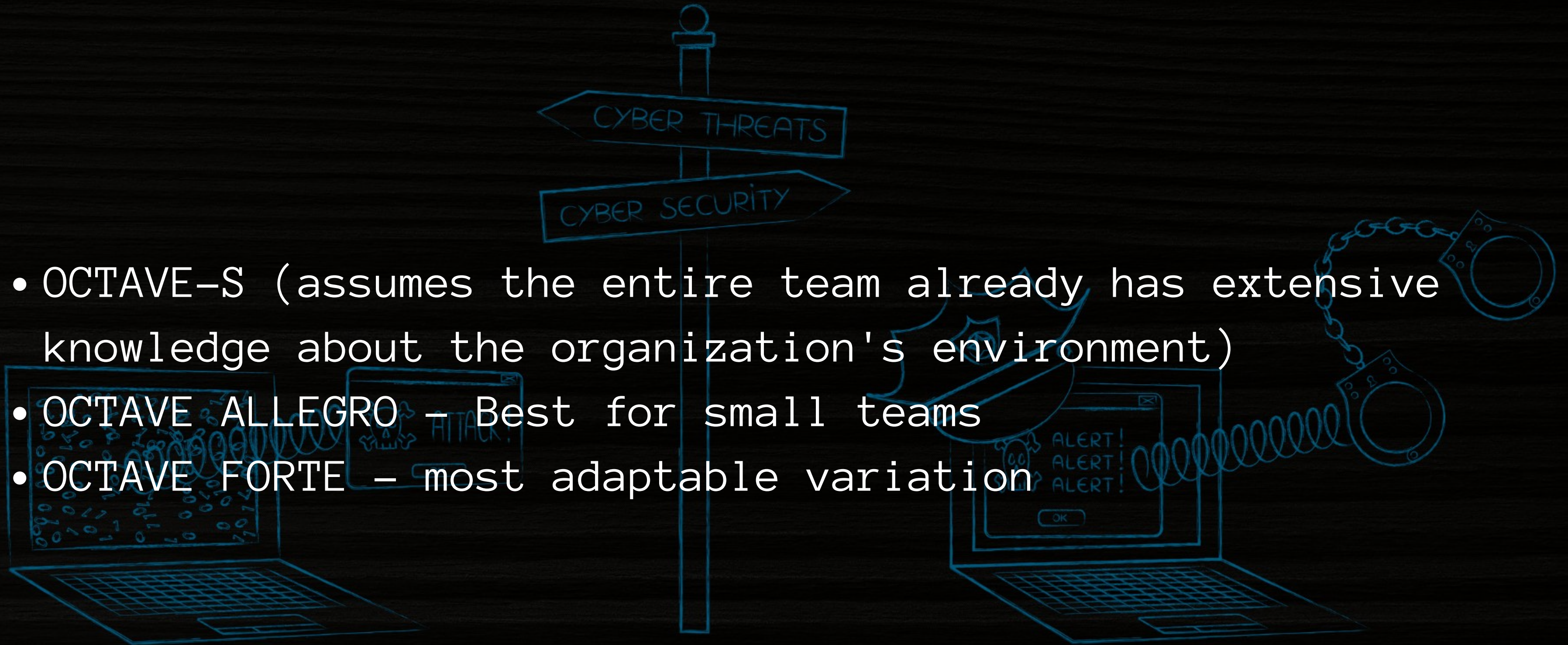
Due to its flexibility, it can be adapted to fit the needs of practically any organization while only requiring a small team of cybersecurity professionals to collaborate on the endeavor.





# OCTAVE

- OCTAVE-S (assumes the entire team already has extensive knowledge about the organization's environment)
- OCTAVE ALLEGRO – Best for small teams
- OCTAVE FORTE – most adaptable variation





# Phases of Implementation





# Phases of Implementation

Identify vulnerabilities and policies should be developed to eliminate and manage them.





# Phases of Implementation

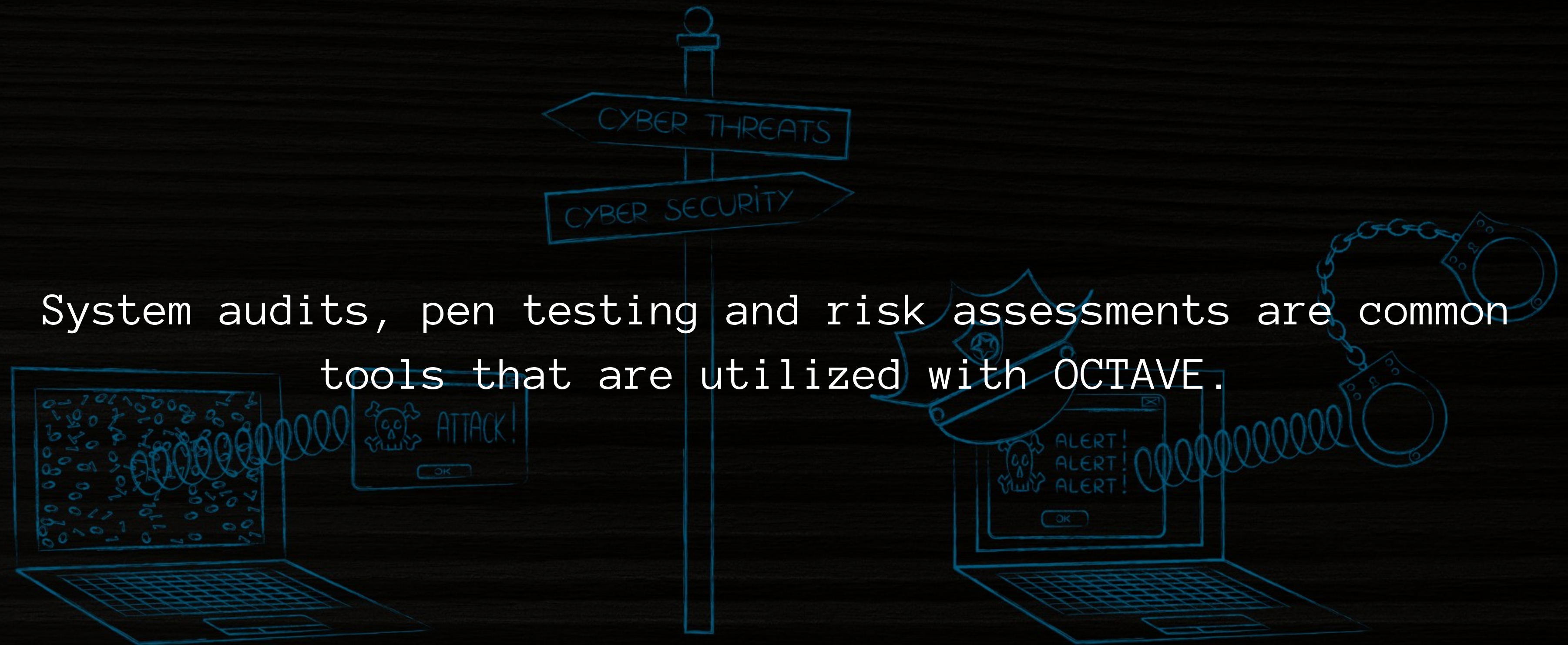


Define a security risk management strategy.





# OCTAVE



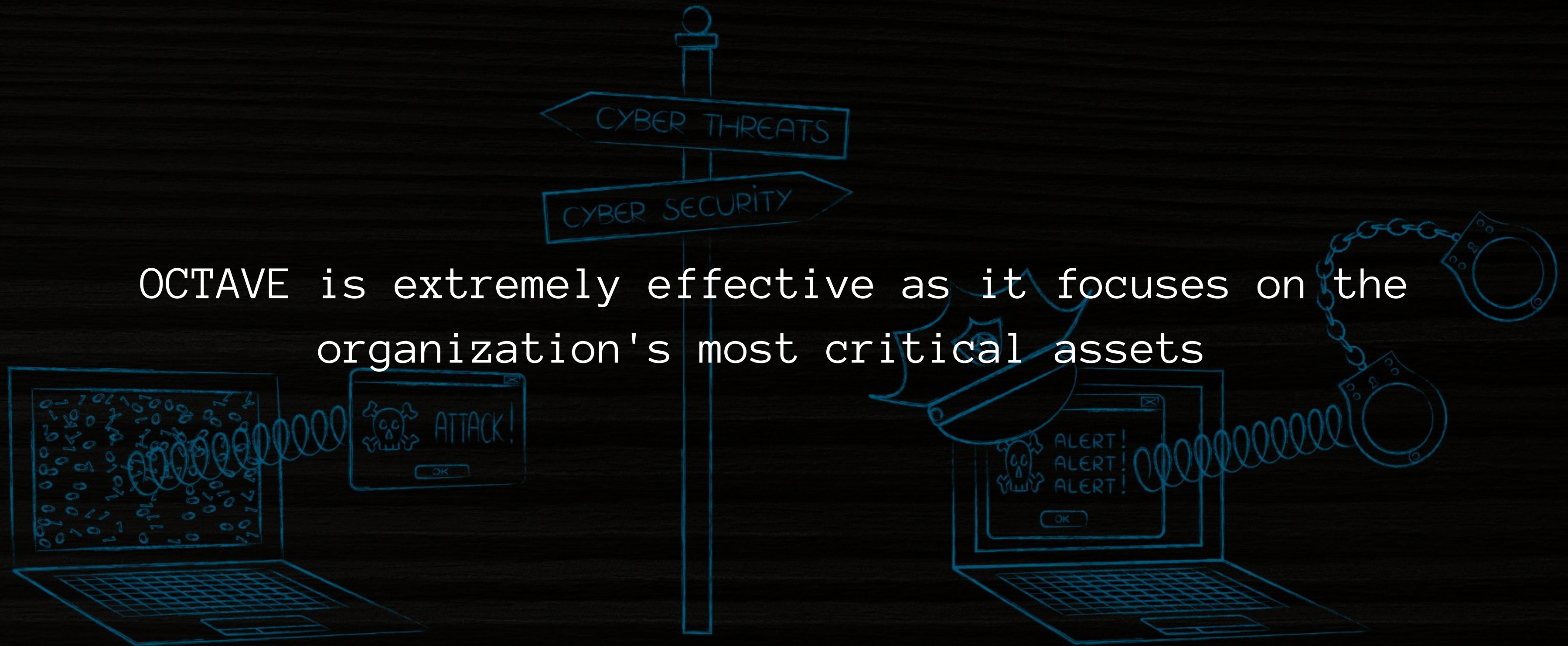
System audits, pen testing and risk assessments are common tools that are utilized with OCTAVE.





# Benefits

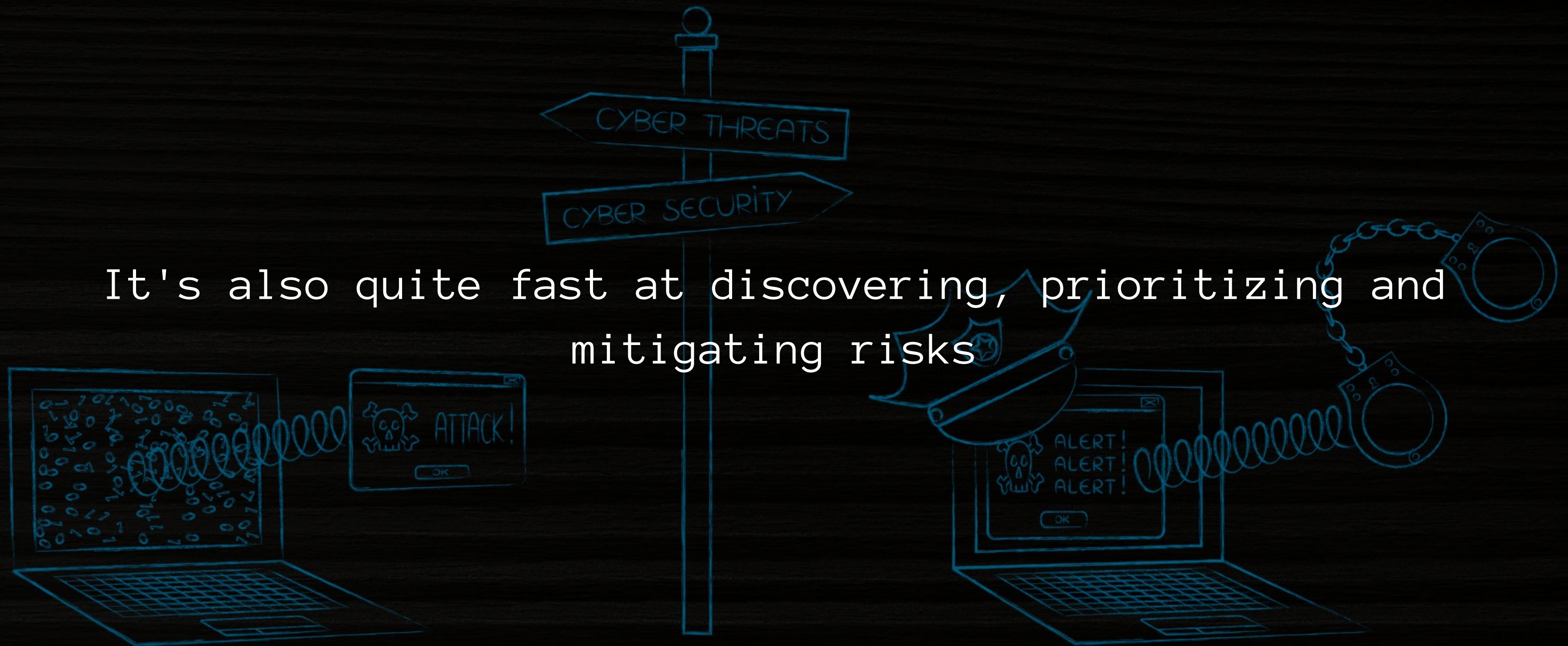
OCTAVE is extremely effective as it focuses on the organization's most critical assets





# Benefits

It's also quite fast at discovering, prioritizing and mitigating risks





# Benefits

It's also actionable and comprehensive

