BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

OPERATIVE PRODUCT WHITEPAPER

BLACKHAWK ALERT OPERATIVE

INTRO

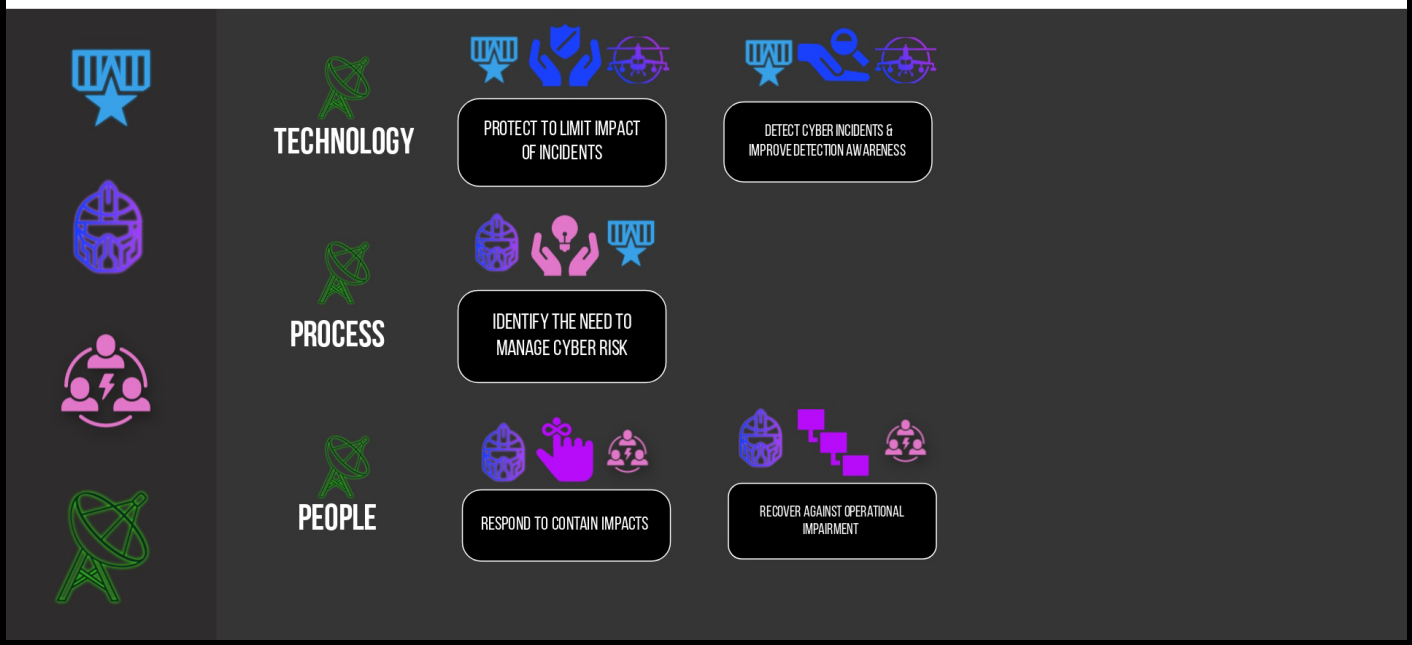
Cybersecurity consulting is the process of providing advice and guidance to organisations on how to secure their networks, systems, and data from cyber threats. Cybersecurity consulting involves sharing knowledge of cybersecurity technologies, policies, and best practices that relate to business operation and technology.

WHAT IS BLACKHAWK OPERATIVE?

Blackhawk Operative is a cybersecurity consulting service that provides our clients a comprehensive cybersecurity strategy regardless of their businesses size. Facilitating such consultation helps to ensure the protection of sensitive data and systems against a rapidly evolving landscape of cyber threats. It also ensures scoping, investment into and implementation of effective processes that are operationally sound.

Our consulting assists businesses adopt frameworks in line with the Essential Eight, NIST and the ACSC's best practice recommendations.

ALIGNMENT TO THE NIST FRAMEWORK

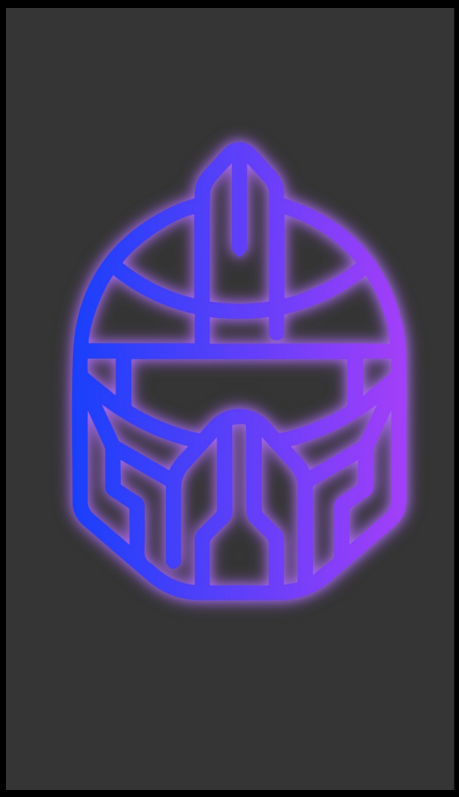


OPERATIVE DEFINITION

As a cybersecurity consulting service, Blackhawk Operative is designed to help organisations identify and mitigate cyber risks. It ensures that businesses have the right systems and processes in place to prevent, detect, and respond to cyber threats. This can include assessments of current security practices, the development of security policies and procedures, the implementation of security technologies, and the planned delivery of training and awareness programs to employees.

Operative consulting can also include crisis management planning, incident response planning, and post-incident analysis to help you effectively manage and recover from security incidents.

KEY FEATURES



BLACKHAWK OPERATIVE SCOPE OF WORK

Creation of cyber risk reports:
seeks to identify the specific cyber threats that your organisation is most vulnerable to and assess the likelihood and impact of these threats.

Risk Management strategy:
develops a risk management strategy that includes measures to prevent, detect, and respond to cyber threats.

Incident response plan:
provides an outline of tailored steps in the event of a cyber attack, including how to contain the damage, investigate the attack, and recover from it.

Security policies and procedures:
present on implementation of security policies and procedures to ensure that all employees understand their roles and responsibilities in maintaining the organisation's security.

Business continuity plan:
assists your business in setting up defined duties and responsibilities to regularly monitor and improve cybersecurity processes and maintenance to stay up-to-date.

Third-party risk management:
Operative consulting can also facilitate risk assessment of that posed by third-party service providers and support implementation measures to manage and mitigate that risk.

BLACKHAWK OPERATIVE INCLUDES A NUMBER OF DIFFERENT AREAS OF CONSULTATION:

- Consulting on Cybersecurity best practices
- Specific considerations based on your business industry and regulations
- Creating a strategy & process to align your organisation to NIST

- Creating a strategy & process to align your organisation to Essential Eight
- Consulting on specific duties and responsibilities relating to processes, people and technology
- Provision of ACSC insights and recommendations

SCOPE OF WORK - CYBER RISK PLANNING

- **Creation of cyber risk reports:**

Blackhawk Operative consulting seeks to identify the specific cyber threats that your organisation is most vulnerable to and assess the likelihood and impact of these threats.

- **Risk Management strategy:**

Consulting through Operative develops a risk management strategy that includes measures to prevent, detect, and respond to cyber threats.

- **Incident response plan:**

As part of Operative consulting, Blackhawk Alert provides your business an outline of tailored steps to take in the event of a cyber attack, including how to contain the damage, investigate the attack, and recover from it.

- **Security policies and procedures:**

In addition to Operative consulting, Blackhawk Alert will also provide and present on a detailed report to revise implementation of security policies and procedures to ensure that all employees understand their roles and responsibilities in maintaining the security of the organisation’s information systems.

- **Business continuity plan:**

Operative consulting can assist your business in setting up defined duties and responsibilities to regularly monitor and improve cybersecurity processes and maintenance to stay up-to-date.

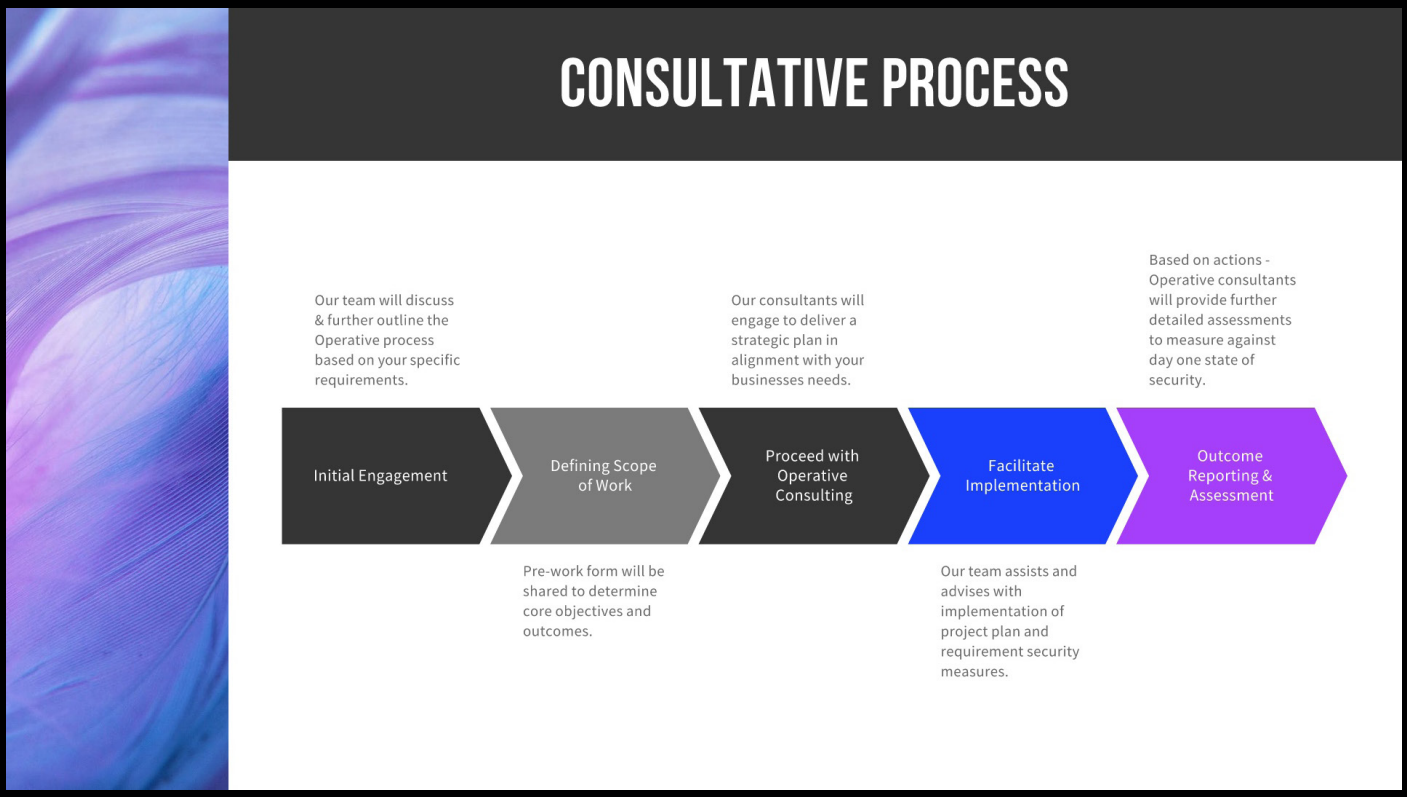
- **Training and awareness:**

Operative consulting can be leveraged to strategise implementation of regular training and awareness programs for employees on cyber security risks and best practices to maintain a secure and informed workforce.

- **Third-party risk management:**

Operative consulting can also facilitate risk assessment of that posed by third-party service providers and support implementation measures to manage and mitigate that risk.

DEPLOYMENT



Deployment for Blackhawk Frontier is incredibly straightforward and seamless.

Blackhawk Alert's service delivery team will remote into your business network in order to install Blackhawk Frontier.

CONCLUSION

Blackhawk Operative is a consulting service that assists with planning and implementing strategies around cyber security.

These strategies implemented ensure:

- Business Continuity Planning
- Employee Best Practice
- Safeguarding of brand reputation
- Protection of sensitive information
- Fulfilment of industry compliance standards
- Harm minimisation from potential, future cyber incidents

Reduce costs by implementing strategies that minimise the likelihood of a breach, stay compliant and drive operational effectiveness of your businesses cybersecurity strategy through Blackhawk Operative.