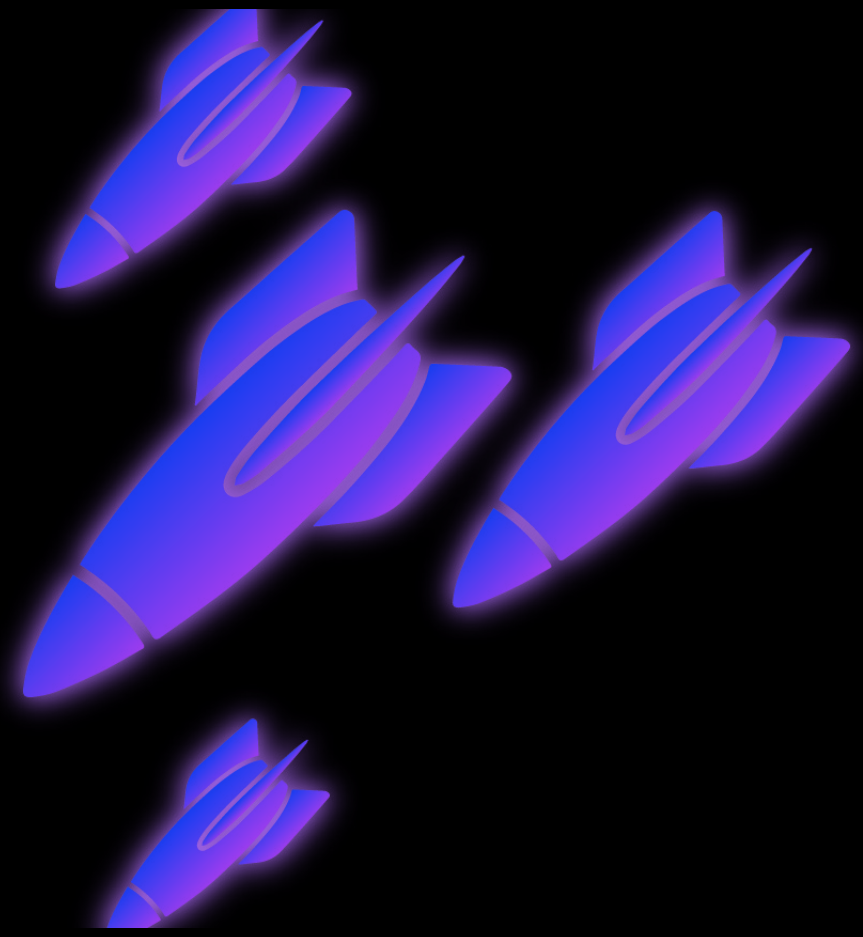
BLACKHAWK ALERT

CYBER SECURITY SOLUTIONS

AIRSTRIKE PRODUCT WHITEPAPER



BLACKHAWK ALERT AIRSTRIKE

INTRO

Blackhawk Alert Airstrike is a bespoke threat response service offered through our security operations team. If through Blackhawk Recon, our assessment detects a live threat in an environment, Blackhawk Alert will ask for authorisation to deploy Blackhawk Airstrike. Our recommendation in such a scenario will always be to neutralise any detected threat as urgently as possible.

WHAT IS BLACKHAWK AIRSTRIKE?

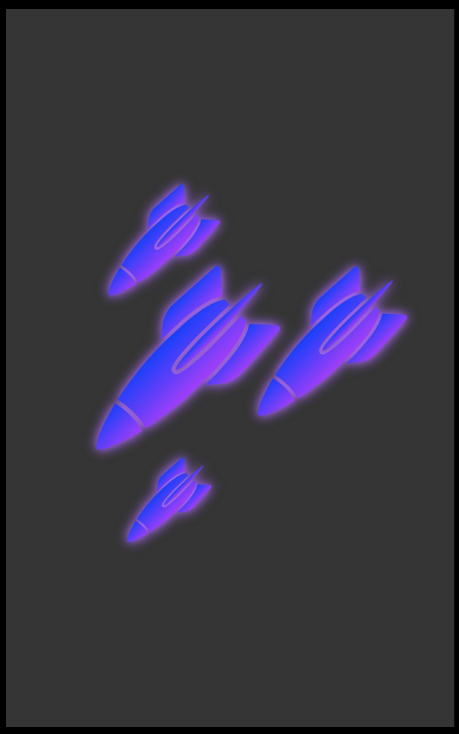
Blackhawk Airstrike is an incident response service utilised after a threat is detected. It involves deploying security analysts in a timely manner to remove a threat to minimise impact of a potential data breach.

As an incident response, Blackhawk Airstrike is used to contain, remove and recover in the aftermath of a detected cyber incident and consequent data breach.

The four key phases of the Blackhawk Airstrike process include:

- Detection
- Preparation and analysis
- Containment and eradication
- Post-incident recovery

KEY FEATURES



BLACKHAWK AIRSTRIKE PROCESS

Detection:
Includes deployment of the Recon assessment to scans systems and networks for indicators of compromise, such as suspicious activity, and alerting if a live threat is detected.

Preparation:
Collaboration to guide and advise on all procedures so that you are informed of the response status . Our designated team is responsible for responding to live threats.

Containment:
This involves Blackhawk Alert's SOC isolating the affected systems and networks to prevent the spread of the incident.

Analysis:
Our SOC collects and analyses data to determine the scope & nature of the contained incident, including what systems were impacted and data which may have been lost or stolen.

Remediation:
Blackhawk Alert's SOC team takes the necessary steps to restore normal operations, including removing the incident cause and repairing any damage.

Recovery:
This involves Blackhawk Alert's SOC restoring any lost data, reconfiguring systems and networks, and performing a post-incident review to identify areas for improvement.

Reporting:
Airstrike completes the response process by sharing reporting on the incident to the appropriate authorities and stakeholders, including law enforcement, regulators, and affected customers or partners.

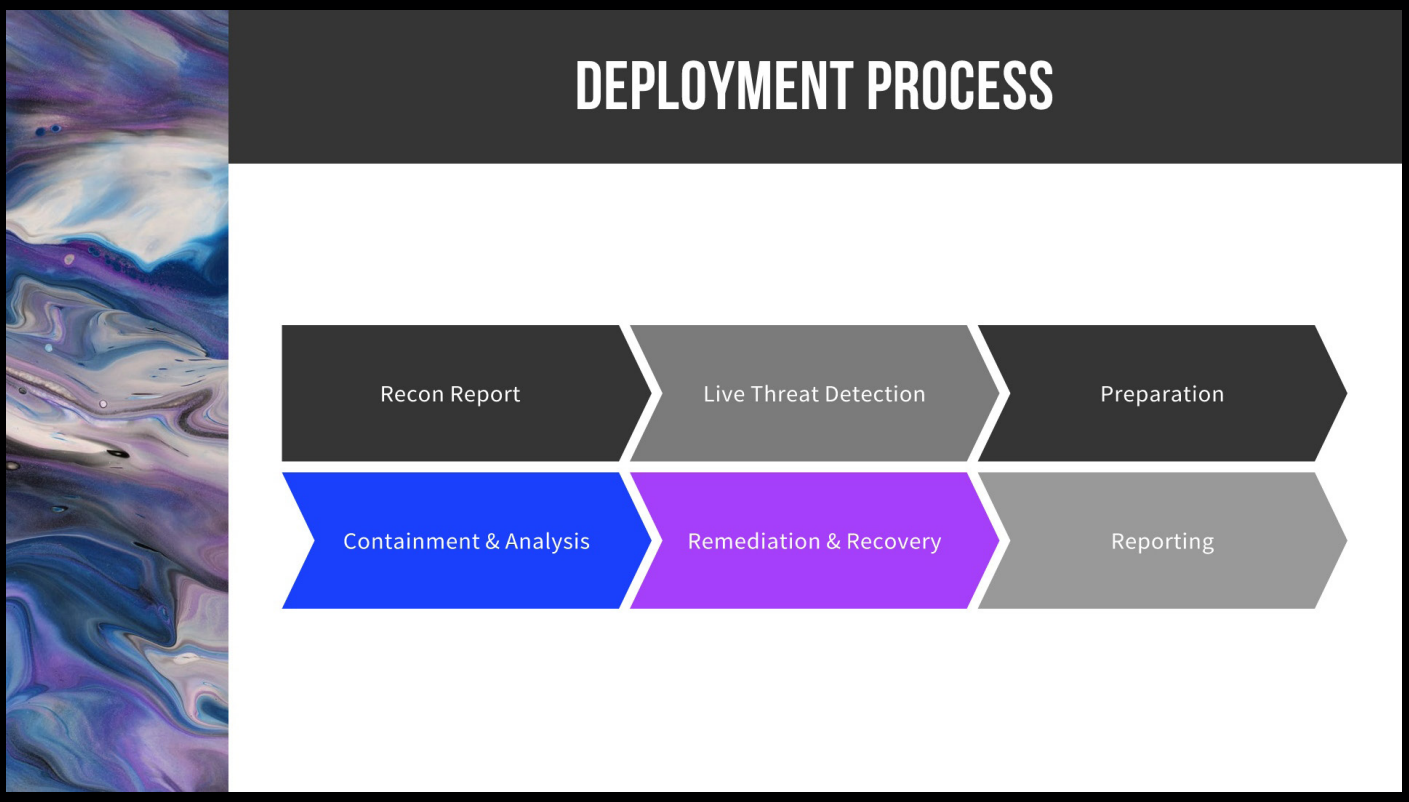
1. **Detection:** The detection phase includes deploying our Recon assessment that scans systems and networks for indicators of compromise, such as suspicious activity, and alerting Blackhawk Alert if a live threat is detected.
2. **Preparation:** This phase relates to Blackhawk Alert's process of collaboration with your business to deliver our strategic response to the detected, live threat. Blackhawk Alert will guide you and advise on all procedures so that you are informed of the status of the response. Blackhawk Alert has a designated team responsible for responding to live threats.
3. **Containment:** This involves Blackhawk Alert's SOC isolating the affected systems and networks to prevent the spread of the incident.
4. **Analysis:** This involves the SOC collecting and analysing data to determine the scope and nature of the incident that has been contained, including what systems were impacted and what data may have been lost or stolen.
5. **Remediation:** Blackhawk Alert's security team takes the necessary steps to restore normal operations, including removing the cause of the incident and repairing any damage.
6. Recovery: This involves Blackhawk Alert's SOC restoring any lost data, reconfiguring systems and networks, and performing a post-incident review to identify areas for improvement.

7. **Reporting:** Airstrike completes the response process by sharing reporting on the incident to the appropriate authorities and stakeholders, including law enforcement, regulators, and affected customers or partners.

DEPLOYMENT

If Blackhawk Recon's assessment detects a live threat within your environment then Blackhawk Alert will recommend an Airstrike be deployed.

Our Security Operations Team will be designated to conduct this cleanup process swiftly to minimise further impact and risk to your business.



CONCLUSION

Blackhawk Airstrike is a treatment of a compromised environment - it minimises the impact of security incidents and data breaches on businesses and their stakeholders, by responding quickly and effectively to minimise damage, reduce recovery time, and prevent future incidents.